Э.Стин

КВАНТОВЫЕ ВЫЧИСЛЕНИЯ

Ижевск: НИЦ «Регулярная и хаотическая динамика», 2000, 112 стр.

Новая область науки о квантовых вычислениях лежит на стыке квантовой теории информации, компьютерных наук и квантовой физики. В небольшом обзоре известного английского специалиста обсуждаются основные понятия квантовых вычислений и квантовой теории информации. Затрагиваются вопросы квантовой криптографии и телепортации.

Книга написана доступно и просто, ориентирована на широкий круг читателей, желающих познакомиться с этой новой и перспективной областью научных исследований.

Содержание

Предисловие

Предмет квантовых вычислений объединяет в себе идеи классической информации, информатики и квантовой физики. В данном обзоре затрагиваются не только квантовые вычисления, но в общих чертах рассматривается вся теория квантовой информации. Информация может рассматриваться как какая-либо структура, движущаяся от причины к следствию. Таким образом, информация имеет фундаментальное значение в физике. Однако математический подход к информации и, в частности, ее обработка возникли совсем недавно — в середине двадцатого века. Таким образом, только сейчас была осознана вся значимость информатики, как основного понятия физики и, в особенности, квантовой механики. Поставив информацию на твердую основу, теория квантовой информации и вычислений привела к более глубокому пониманию окружающего мира. Были найдены: защищенный способ переноса классической информации с помощью квантовых состояний (квантовая криптография), надежный метод переноса квантовых состояний, посредством квантового зацепления (телепортация), возможность сохранения квантовой когерентности при необратимых шумовых процессах (исследование квантовых ошибок) и метод эффективных квантовых вычислений посредством контролируемой квантовой эволюции. Идея, объединяющая данные открытия, заключается в использовании квантового зацепления в качестве вычислительного средства.

Становится ясно, что теория информации и квантовая механика хорошо дополняют друг друга. Для объяснения их взаимосвязи обзор начинается со вступления в классическую теорию информации и в информатику. Там же рассматривается теорема Шеннона, коды, исправляющие ошибки, машина Тьюринга и сложность вычислений. После этого даются основные принципы квантовой механики и описание эксперимента EPR (Einstein–Podolski–Rosen). Корреляции EPR-Bell и квантовое зацепление проводят линию раздела между квантовой и классической теорией информации и, возможно, между квантовой и классической физикой.

В дальнейшем в общих чертах обозначаются основные идеи по работе с квантовой информацией: сжатие кубитов и информации, квантовые логические гейты, свойство неклонируемости неизвестного квантового состояния (no cloning property) и телепортация. Вкратце рассматривается квантовая криптография. Дается описание универсального квантового компьютера, опирающееся на принцип Чёрча – Тьюринга и сетевую модель вычислений. Рассматриваются алгоритмы для данного компьютера, в частности, алгоритмы поиска периода функции и поиска записи в неупорядоченной базе данных. Эти алгоритмы показывают, что квантовый компьютер, обладающий достаточно точной структурой, не только существенно отличается от любого другого компьютера, оперирующего классической информацией, но способен обрабатывать малый класс функций с более высокой производительностью. Это значит, что для некоторых важных вычислительных задач требуется только квантовый компьютер.

Для создания универсального квантового компьютера требуются технологии даже не завтрашнего дня. Однако принципы физики квантовой информации могут быть проверены на более скромных устройствах. В дальнейшем будет проведен обзор создавшегося положения в отношении экспериментов. Особо отмечаются методы применения линейной ионной ловушки, высококачественных оптических резонаторов, а также метод ядерного магнитного резонанса. Вышеуказанные устройства и методы обеспечивают связное управление в восьмимерном гильбертовом пространстве (определяется тремя кубитами); однако область их применения может быть расширена до тысячи и более мерных пространств (определяются десятью кубитами). Кроме того, данные системы (устройства) позволяют определить осуществимость квантовых вычислений. Поскольку на практике такие эксперименты трудно осуществимы, а также из соображений их неточности и неизбежного взаимодействия любой системы с окружающей средой, то до недавнего времени возможность создания действующего квантового компьютера (оперирующего примерно 1000 кубитами) была исключена. Однако подраздел физики квантовой информации предлагает метод исправления квантовых ошибок (QEC — quantum error correction) как решение данной проблемы.

Проводится ознакомление с методом исправления квантовых ошибок. Эволюция квантового компьютера ограничена рамками тщательно выбранного подпространства в его гильбертовом пространстве. Ошиб-

ки с большой вероятностью могут вызвать отклонение от данного подпространства. С помощью метода QEC становится возможным обнаружение и исправление таких отклонений без нарушения квантового вычисления. Этим достигается практически невозможное, поскольку вычисление не нарушает квантовой когерентности, хотя в ходе самого вычисления все кубиты в компьютере будет релаксировать одновременно по многу раз.

Обзор завершается выводом по основным свойствам физики квантовой информации и по перспективным направлениям для исследований.

Глава 1
Введение

Физика старается задать и получить точный ответ на основной вопрос: почему окружающий нас мир такой, какой он есть. Исторически, фундаментальные законы физики были связаны с такими вопросами, как: «Из чего состоят тела?» или «Почему тела движутся так, а не иначе?». Ньютон в своей работе *Principia* дал очень общие ответы на некоторые из вопросов. Он показал, что движение как обычных предметов, так и планет описывается одними и теми же математическими уравнениями и сделал вывод, что такое тело, как заварочный чайник имеет то же строение вещества, что и планета: их движения определяются массой и силами, действующими на них. Сегодня можно сказать, что движение этих двух тел подчиняется закону сохранения энергии и количества движения. Таким образом, физика позволяет абстрагироваться от таких природных понятий, как энергия или импульсы, которые всегда описываются низменными уравнениями. Хотя одна и та же энергия может быть выражена различными способами: например, электрон в большом электрон-позитронном коллайдере CERN (Женева) обладает такой же кинетической энергией, что и слизень на листе салата.

Другим понятием, которое также может быть выражено различными способами, является информация. Например, два предложения «квантовый компьютер представляет интерес» и «l'ordinateur quantique est trés intéressant» в чем-то совпадают, но содержат разные слова. Их общее место есть информационное содержание. Очень важным является то, что одна и та же информация может быть представлена различными способами. Например, заменяя буквы на цифры следующим образом: $a \to 97$, $b \to 98$, $c \to 99$ и т. д., английский вариант вышеуказанного утверждения будет выглядеть так: 116 104 101 32 113 117... Важно то, что существует возможность автоматизированного оперирования информацией, поскольку различные способы ее представления не изменяют содержания: от компьютера для обработки больших объемов информации, начиная подготовкой документа и заканчивая дифференциальными вычислениями и переводом с одного языка на другой,

требуется лишь способность оперировать такими довольно простыми величинами, как целые числа.

Сейчас такие утверждения кажутся привычными, но еще 50 лет назад никто не мог предвидеть подобного распространения автоматической обработки информации (информационных технологий).

Однако все способы представления информации совпадают в одном: их использование основано на каком-либо физическом явлении. Так устная речь передается за счет колебаний давления воздуха, письменная речь — за счет определенного расположения молекул чернил на бумаге и даже мыслительный процесс определяется работой нейронов (Landauer 1991). Как говорят физики: «Любая информация имеет физическое представление». Наоборот, поскольку информация не зависит от вида ее представления и может быть легко переведена из одного вида в другой, она, очевидно, может войти в ряд фундаментальных понятий физики, таких, как энергия, импульс и другие. Однако точный математический аппарат, описывающий информацию и, в частности, ее обработку, отсутствовал до второй половины этого столетия. Поэтому важность информации для физики лишь слегка обозначалась в таком понятии термодинамики, как энтропия. Сегодня становится понятным, что информация имеет гораздо большее значение. Исторически сложилось так, что большинство фундаментальных физических наук занимались поиском элементарных частиц и уравнений, описывающих их движение и взаимосвязи. Сегодня появляются не менее важные цели: поиск способов, подходящих для представления информации и оперирования ею. Например, для определения того, что может или не может двигаться быстрее скорости света, необходимо охарактеризовать информацию как ограниченный по скорости света объект. В квантовой механике очень важно, чтобы вектор не содержал (явно или неявно) *больше информации, чем может быть связано с данной системой*. Кроме всего прочего, это приводит к условию симметрии волновой функции, что в свою очередь приводит к статистике Бозе–Эйнштейна и Ферми–Дирака, периодичной структуре атомов и др.

Идея пересмотра фундаментальных физических свойств с точки зрения теории информации появилась совсем недавно. Однако она уже приносит плоды и именно этой перспективной задаче посвящен данный обзор.

Исторически точное время появления понятия информации в физике не определено. Важным событием в теории может считаться по-

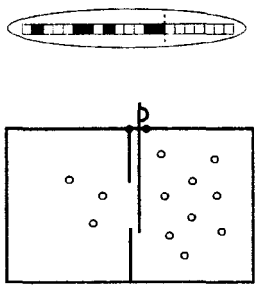

Рис. 1. Демон Максвелла. На данном рисунке показано, что демон создает разницу давлений путем открывания перегородки только в том случае, когда к ней слева приближается молекул больше, чем справа. Пока демон способен хранить в памяти результаты наблюдений относительно молекул, данные действия полностью обратимы. Однако при этом голова (память) демона нагревается. Шаг необратимости заключается не в приобретении информации, а в ее потере при очистке демоном своей памяти

явление в 1871 году парадокса, называемого «демон Максвелла» (рис. 1, см. также Brillouin, 1956 г.). Демон Максвелла — это такое существо, которое отделяет быстрые молекулы от медленных (или горячие от холодных). Таким образом, его действия приводят к возникновению разницы температур без совершения какой-либо работы, что нарушает второй закон термодинамики и приводит к множеству противоречий. Существовало множество попыток «изгнать» демона Максвелла (объяснить парадокс Максвелла) (см. Bennett 1987): утверждалось, что демон не может получать информацию без совершения работы, либо без возмущения (и, следовательно, нагрева) вещества. Как первое, так и второе утверждения неверны. Кое-кто поддался искушению объявить о том, что второй закон термодинамики действительно может быть нарушен «мыслящим (разумным) существом». Определенный процесс наметился только в 1929 г., когда Лео Сциллард свел задачу к ее основным составляющим, где демону требовалось лишь определить: находится ли молекула слева или справа от перегородки. Действия демона обеспечивают работу простого теплового двигателя, называемого двигателем Сциларда.

Однако Сциллард не решил задачу, поскольку его анализ не объяснял, будет ли акт измерения, посредством которого демон узнает о положении молекулы, способствовать увеличению энтропии.

Удивительно, но окончательный ясный ответ появился лишь через пятьдесят лет. В течение этого периода были разработаны цифровые компьютеры, а также были тщательно изучены с физической точки зрения сбор и обработка информации. Вклад термодинамики в оперирование элементарными объемами информации изучался Ландауэром и другими в 60-х годах, а ее вклад в вычисления — Беннеттом, Фредкином, Тоффоли и другими в 70-х годах. Было замечено, что почти любой процесс является обратимым, т. е. для него не существует энтропии (Bennett and Landauer, 1985 г.). Беннетт ясно определил связь между этой работой и парадоксом Максвелла, полагая, что демон в действительности может определить положение молекулы в двигателе Сцилларда, не совершая работы и без увеличения энтропии в окружающей среде. Таким образом, за один цикл работы двигателя приобретается полезная работа. Однако в этом случае информация о положении молекулы должна находиться в памяти демона (рис. 1). Чем больше циклов работы двигателя выполнено, тем больше информации накапливается в его памяти. Для завершения термодинамического цикла демон должен очистить свою память. Именно этот процесс удаления информации связан с увеличением энтропии в окружающей среде, чего и требует второй закон термодинамики. На этом завершается рассмотрение физической сути демона Максвелла. Более тонкое обсуждение этого парадокса можно найти у Zurek (1989), Caves (1990), Caves, Unruh and Zurek (1990).

Вышеописанный пример поучителен. Полное же описание исторического проявления идей, связанных с квантовыми вычислениями, является грандиозной задачей. Данный предмет охватывает два, возможно, величайших открытия, стоящих в ряду революционных открытий науки XX века: квантовую механику и теорию информации (в том числе информатику). Взаимосвязь этих двух гигантов показана на рис. 2.

В основе классической теории информации лежит определение непосредственно информации. Здесь уместно следующее предупреждение. Как только теория пытается из термина «информация» вытеснить, насколько это возможно, естественный смысл этого понятия, она больше не может оценить всю полноту этого слова в его повседневном понимании и видит в нем не больше, чем физика элементарных частиц видит в понятии «очарование». Пока будем считать понятие «информация» абстрактным. Его точное определение будет дано в разделе 2.1. Большинство понятий теории информации относится к 1940 году — времени

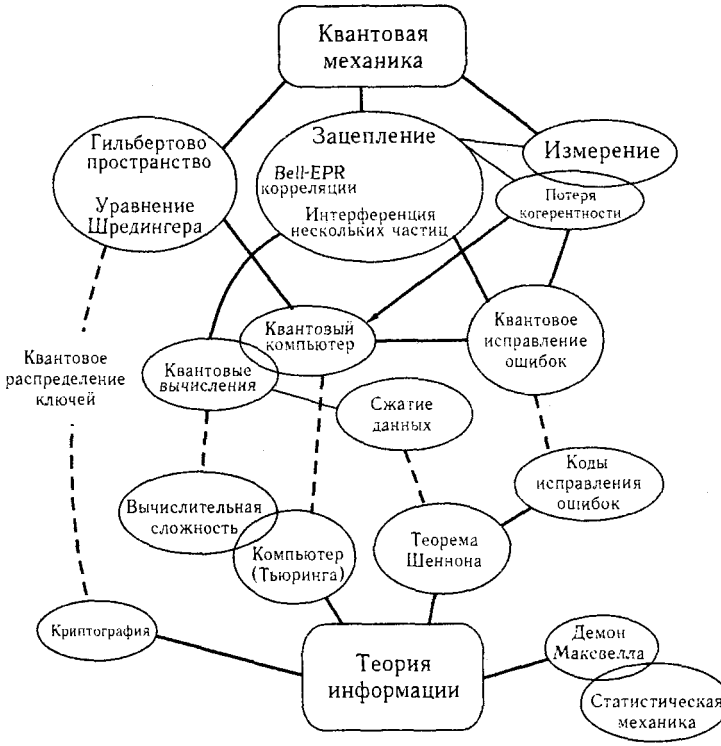

Рис. 2. Зависимость между квантовой механикой и теорией информации. Данная диаграмма не претендует на роль определения, поскольку расположение элементов в некотором роде субъективно. Однако она указывает на многие связи, описанные в статье

появления основополагающей работы Шеннона (Slepian 1974 г.). Данные о том, что информация может быть преобразована из одной формы в другую, кратко изложены и квантифицированы в теореме бесшумного кодирования Шеннона (Shannon's noiseless coding theorem).

Эта теорема количественно определяет средства, необходимые для хранения или передачи заданного объема информации. Шеннон также рассмотрел фундаментальную задачу о связи при помехах и вывел основную теорему Шеннона (см. раздел 2.4), которая является важным достижением классической теории информации. Связь без ошибок даже

при помехах осуществляется посредством «кодов, исправляющих ошибки», изучением которых по праву занимается одна из ветвей математики. Журнал IEEE Transactions on Informations Theory практически полностью посвящен разработке и анализу кодов, исправляющих ошибки. Новаторские работы в этой области были выполнены Golay (1949) и Hamming (1950).

Основные положения информатики появились примерно в то же время, что и теория информации Шеннона. Данный факт не является совпадением. Можно утверждать, что Алан Тьюринг (Alan Turing 1912–1954) — отец информатики, а пророк ее — Чарльз Бэббидж (Charles Babbage 1791–1871). Бэббидж определил большинство существенных элементов современного компьютера, хотя в то время еще не существовало технологий для осуществления его идей. Прошло столетие и Тьюринг усовершенствовал «аналитическую машину» Бэббиджа, предложив в середине 30-х годов универсальную машину Тьюринга. Гений Тьюринга (см. Hodges 1983) заключается в том, что он точно определил возможности вычислительной машины и в еще большей степени, чем Бэббидж, подчеркивал роль программирования или, другими словами, программного обеспечения. В своих исследованиях Тьюринг опирался на работы таких великих математиков, как Дэвид Гильберт и Курт Гедель. С 1890-х по 1930-е годы Гильберт подчеркивал важность постановки фундаментальных вопросов о природе математики. Вопрос: «Справедливо ли данное математическое утверждение?» он предлагал заменить вопросом: «Можно ли данным способом в принципе опровергнуть или доказать любое математическое утверждение?» Ответ был неизвестен, однако Гильберт, как и большинство математиков, чувствовал, что математика является законченной наукой и такие предположения, как, например, предположение Гольдбаха о том, что любое четное число можно представить как сумму двух простых чисел, могут быть либо доказаны, либо опровергнуты. Хотя логическая последовательность доказательств может быть и неизвестна.

Гедель опровергнул эти идеи, доказав существование неразрешимых математических утверждений, т. е. утверждений, которые нельзя ни доказать, ни опровергнуть. Следующий важный вопрос был связан с опознаванием подобных утверждений. Прогресс математики всегда зависел от гибкости воображения, однако при суждении задним числом математические доказательства выводятся автоматически, где каждый последующий шаг неизбежно следует из предыдущего. Гильберт

задавался вопросом, можно ли заменить эту «неизбежность» каким-либо автоматическим процессом. Другими словами, существует ли универсальный математический метод, позволяющий доказать истинность или ложность любого математического утверждения? После Геделя вопрос Гильберта был переформулирован. Теперь он заключался в доказательстве не истины, а разрешимости, и именно этим вопросом занимался Тьюринг.

По словам Ньюмана, смелость идеи Тьюринга заключалась в изобретении бумажной перфоленты с символической логикой. Во время поиска автоматических действий для разрешения математических вопросов Тьюринг придумал полностью механическое устройство, являющееся фактически всем известной пишущей машинкой (рис. 7, стр. 39). Особенность машины Тьюринга заключалась в том, что, с одной стороны, это была машина высокого уровня, предназначенная для решения сложных математических задач, с другой стороны, она была достаточно проста и могла быть подвергнута подробному анализу. Тьюринг использовал свою машину как теоретическую конструкцию для того, чтобы доказать, что допущения существования механических средств для доказательства разрешимости ведет к противоречию (см. раздел 3.3). Другими словами, он изначально занимался довольно абстрактной математикой, а не практическими вычислениями. Однако серьезно подходя к идее автоматического математического доказательства, а не к идее простых расчетов, Тьюринг значительно способствовал развитию обработки информации общего назначения. Это было время, когда, говоря «компьютер», подразумевали «занимающийся математикой».

Современные компьютеры не являются ни машинами Тьюринга, ни машинами Бэббиджа, хотя и имеют много общего. А их вычислительная мощность эквивалентна (в техническом смысле) мощности машины Тьюринга. Несмотря на то, что это было бы занимательно, здесь не описывается история развития компьютеров, поскольку пришлось бы упоминать вклад очень многих людей. Следует отметить, что весь процесс развития затрагивает лишь размеры и быстродействие, но не касается основных принципов структуры или работы компьютера. Однако квантовая механика ставит вопрос о возможности подобных изменений.

Квантовая механика — это математическая структура, которая, в принципе, охватывает всю физику. Здесь не будут на прямую рассматриваться гравитация, высокие скорости или необыкновенные эле-

ментарные частицы, поэтому знаний нерелятивистской квантовой механики будет достаточно. Важной чертой квантовой механики является не точное описание уравнений движения, а тот факт, что эти уравнения оперируют не классическими переменными, а квантовыми амплитудами или векторами в гильбертовом пространстве. Именно это способствует появлению новых видов информации и вычислений.

Существует параллель между вопросами Гильберта о математике и вопросами, которые стараются сформулировать перед квантовой теорией информации. До Гильберта практически все математические работы были связаны с доказательством либо опровержением некоторых гипотез. Однако Гильберт пытался определить общий вид гипотезы, поддающийся математическому доказательству. Подобным образом большинство исследований в квантовой физике были связаны с изучением эволюции отдельных физических систем, хотя требуется определить общий вид эволюции, возможный при каких либо квантовомеханических условиях. Первое глубокое осознание квантовой теории информации возникло с появлением в 1964 г. анализа Белла (Bell), проведенного им в отношение парадоксального мысленного эксперимента, который был предложен в 1935 году Эйнштейном, Подольски (Podolski) и Розеном (Rosen) (EPR). Неравенство Белла обращает внимание на важность корреляции между отдельными квантовыми системами, которые в прошлом взаимодействовали (прямо или косвенно) между собой, но больше не воздействуют друг на друга. В сущности его аргументы показывают, что практический уровень корреляции в подобных системах превышает теоретический уровень, определяемый на основании любого закона физики, описывающего появление частиц с помощью классических переменных, а не квантовых состояний. Аргументы Белла были уточнены Bohm (1951 г., также Bohm and Aharonov, 1957 г.) и Clauser, Holt and Shimony (1969), а в 70-х были проведены эксперименты (см. Clauser and Shimony (1978) и ссылки там же). Главная ценность этих экспериментов заключается в возможности какого-либо взаимодействия между обособленными квантовыми системами. Значительный прогресс был достигнут в эксперименте Aspect, Dalibard and Roger (1982) (см. также Aspect, 1991), где любое, имеющее смысл взаимодействие либо имеет скорость, превышающую световую, либо обладает другими, почти неправдоподобными свойствами.

Следующее звено между квантовой механикой и теорией информации возникло после осознания того факта, что такие простые свойства

квантовых систем, как неизбежное их нарушение при измерениях могут использоваться на практике в квантовой криптографии (Wiesner, 1983, Bennett et. al., 1982, Bennett and Brassard 1984, последние отчеты: Brassard and Crepeau 1996). Квантовая криптография объединяет несколько идей, из которых неизменной является идея квантового протокола передачи кода. Это несложный метод, где передаваемые квантовые состояния используются для выполнения совершенно особенной задачи связи: установить в двух отстоящих друг от друга точках пару идентичных, но, с другой стороны, случайных последовательностей двоичных цифр так, чтобы они (последовательности) оставались неизвестны для третьего лица. Этот метод очень полезен, поскольку подобная случайная последовательность может использоваться как криптографический код для обеспечения защищенной связи. Важной особенностью здесь является то, что принципы квантовой механики обеспечивают такой вид сохранения квантовой информации, что при поступлении необходимой квантовой информации к сторонам, желающим установить случайный код, эти стороны могут быть уверены, что информация не поступила к кому-либо еще (например, шпиону). Таким образом, используя преимущества строения (структуры) окружающего мира, можно легко избежать проблемы шантажа с целью получения кода, которая встречается в анналах шпионажа.

В то время, пока анализировалась и демонстрировалась квантовая криптография, на свет незаметно появился квантовый компьютер. В поведении всех систем, даже тех, которые называются классическими, лежит квантовая механика. («Даже отвертка является квантово-механической системой» — Landauer, 1995 г.) Несмотря на это, было сложно представить квантово-механический компьютер, который воспроизводил бы метод работы машины Тьюринга. Очевидно, недостаточно просто охарактеризовать квантово-механическую систему, чья эволюция может рассматриваться как вычисление — необходимо более серьезное доказательство. С другой стороны, известно, что классические компьютеры могут имитировать посредством вычислений эволюцию любой квантовой системы. Здесь есть одно «но»: ни один классический процесс не позволяет создавать разделенные системы, корреляция которых не подчиняется неравенству Белла. Из этого следует, что корреляции EPR-Bell являются основным квантово-механическим свойством (Feyman 1982 г.).

Первые идеи рассмотрения вычислений с квантово-механической

точки зрения заключались в преобразовании работы машины Тьюринга к эквивалентному обратимому процессу и содержали новое понятие — гамильтониан, способствовавший такой эволюции квантовой системы, которая копировала бы обратимую машину Тьюринга. Эти идеи появились благодаря работе Bennett (1973 г., см. также Lecerf 1963 г.), в которой он показал, что универсальная классическая вычислительная машина (такая, как машина Тьюринга) может быть обратимой, без потери своей простоты. Benioff (1980, 1982) и другие предложили подобные гамильтонианы типа Тьюринга в начале 80-х годов. Хотя идеи Бенёва не позволяли провести полный анализ квантового вычисления, они показывали, что унитарная (единичная) квантовая эволюция по крайней мере обладает такой же вычислительной мощностью, что и классический компьютер.

Другого подхода придерживался Feyman (1982, 1986). Он рассматривал возможность создания не универсального вычисления, а универсальной имитации — специально созданной квантовой системы, способной имитировать физическое поведение любой другой системы. Очевидно, что таким имитатором может быть и универсальный компьютер, поскольку любой компьютер является физической системой. Фейнман привел доводы, из которых следовало, что квантовая эволюция может более эффективно, чем любой классический компьютер, использоваться для решения определенного типа задач. Но его устройство не могло быть названо компьютером, поскольку схема его функционирования была определена не полностью: он предположил, что можно определить порядок любого взаимодействия между смежными системами с двумя состояниями, но не объяснил, как определить этот порядок.

Следующее важное открытие было сделано Дойчем в 1985 году. Его предложение можно рассматривать как первую приближенную схему работы квантового компьютера. Хотя следующее утверждение является спорным, но в силу своей специфичности и простоты, данная схема может являться схемой действия реального устройства, а в силу своей гибкости она может описывать работу и универсального компьютера. По своей сути система Дойча представляет собой ряд систем с двумя базисными состояниями и больше похожа на регистровую машину, чем на машину Тьюринга (обе машины являются универсальными классическими вычислительными машинами). Дойч доказал, что можно получить любую единичную эволюцию, а следовательно, реализо-

вать эволюцию, имитирующую развитие любой физической системы, если возможно осуществить эволюцию системы с двумя состояниями посредством определенного малого множества простых операций. Опираясь на вышеизложенные идеи, Дойч также описал создание режима работы, сходного с функционированием машины Тьюринга.

Сегодня простые операции, предложенные Дойчем, называются квантовыми «гейтами», поскольку их назначение аналогично назначению двоичных комплексных гейтов в классических компьютерах. Разными авторами был предложен наименьший класс гейтов, достаточный для проведения квантовых вычислений.

Однако есть два спорных аспекта в проекте Дойча: его производительность (эффективность) и осуществимость. Вопрос эффективности является фундаментальным в информатике, и на нем строится понятие «универсальность». Универсальным компьютером называется такой компьютер, который не только воспроизводит (имитирует) работу любого другого, но и делает это достаточно быстро. Здесь выражение «достаточно быстро» определяется посредством требуемых для вычисления шагов: их количество не должно зависеть экспоненциально от размера входных данных (точное значение будет дано в разделе 3.1). С этой точки зрения имитатор Дойча не является универсальным. Ллойд показал, что он может быть эффективным при имитации широкого класса квантовых систем (1996). В своей работе Дойч также дает определение квантовых сетей (Deutsch, 1989) и квантовых технических гейтов. Последние имеют огромное значение, поскольку позволяют напрямую говорить о квантовом вычислении.

В начале 1990-х годов несколько авторов (Deutsch и Jazsa, 1992, Berthiaume and Brassard, 1992, Bernstein и Vazirani, 1993) занимались поиском задач, чье решение с помощью квантового компьютера было бы более эффективно, чем их решение посредством любого классического компьютера. При определении каких-либо понятий, относящихся к основам квантовой механики, подобный квантовый алгоритм может играть такую же основополагающую роль, что и неравенство Белла. Первоначально были обнаружены лишь небольшие различия в работе (алгоритмов): в случае, когда квантовая механика при условии, что на квантовую систему не действуют помехи, могла дать определенный ответ — вероятностный классический компьютер мог получить тот же ответ только с высокой вероятностью. Симон (Simon) в 1994 году сделал важное открытие, описав эффективный квантовый алгоритм

для решения (в некотором смысле абстрактной) задачи, не имеющей классических эффективных решений даже при использовании вероятностных методов. Это открытие вдохновило Шора (Shor), и он поразил общественность, когда в 1994 году описал алгоритм, который был не только эффективен при его реализации на квантовом компьютере, но также был адресован для решения основной задачи информатики: разложению на множители простых целых чисел.

Шор, применяя метод квантового Фурье-преобразования, открытый Копперсмитом (Coppersmith) и Дойчем, описал как разложение на множители, так и дискретные логарифмы. Другие важные квантовые алгоритмы были описаны Гровером (Grover, 1997) и Китаевым (Kitaev, 1995).

Как и в случае с классическими вычислениями и теорией информации, при появлении идей, теоретически описывающих вычисления, возникла попытка определения основ квантовой информации — задача, сходная с работой Шеннона. Сложность здесь может заключаться в рассмотрении такой простейшей квантовой системы, как спина-$\frac{1}{2}$ в магнитном поле (система с двумя состояниями). Квантовое состояние спина есть непрерывная величина, определяемая двумя вещественными числами и, в принципе, способная хранить бесконечное количество классической информации. Однако измерение спина дает лишь одно число, способное принимать два значения («спин вверх», «спин вниз»), и, таким образом, не существует какого-либо способа доступа к тому бесконечному объему информации, который должен храниться данным квантовым состоянием. Следовательно, будет некорректным давать хранимой информации подобное определение. Все вышесказанное схоже с задачей перенормировки в квантовой электродинамике. В таком случае, какой объем информации может хранить квантовая система с двумя состояниями? Ответ, предложенный Jozca and Schumacher (1995), заключался в том, что информация, содержащаяся в системе с двумя состояниями, может использоваться как единица измерения! Разумеется, Шумахер и Джозса не только предложили этот простой ответ, но и показали, что системы с двумя состояниями имеют то же значение в квантовой теории информации, что и бит в классической теории информации. Они также показали, что объем квантовой информации, содержащийся в любой квантовой системе, может быть выражен минимальным числом систем с двумя состояниями — называе-

мыми теперь квантовыми битами или кубитами, и которые необходимы для хранения или передачи с высокой точностью состояния системы. Здесь нужно вернуться к вопросу об осуществимости квантового вычисления. Существует простое, но имеющее фундаментальное значение наблюдение, заключающееся в том, что эффект квантовой интерференции, которая обеспечивает функционирование алгоритмов, подобных алгоритму Шора, является очень хрупким: квантовый компьютер очень чутко реагирует на помехи при эксперименте и прочие воздействия.

Было бы неверным полагать, что первые разработчики не знали о существовании этой проблемы. Но их главная цель заключалась в доказательстве (или опровержении) фундаментального значения квантового компьютера. Опираясь на алгоритм Шора, это фундаментальное значение можно считать доказанным посредством следующего аргумента: либо природа допускает существование устройства, работающего с точностью, достаточной для реализации алгоритма Шора для больших чисел (больших, чем, скажем, гугол (googol) (10^{100})), либо существует фундаментальное естественное ограничение точности для реальных систем. Оба возможных случая представляют собой существенное продвижение в изучении законов природы.

На данном этапе происходит объединение квантовой теории информации и теории квантовых вычислений. Причина в том, что можно снизить чувствительность квантового компьютера к шумовым помехам с помощью нового метода, полученного непосредственно вследствие объединения квантовой механики и классической теории информации: метода исправления квантовых ошибок. Хоты выражение «исправление ошибки» используется давно и применялось к квантовым компьютерам раньше, только в 1996 году, благодаря работам Калдербанка (Calderbank) и Шора, а также независимо от них, работе Стина, была создана общая система кодирования, которая позволяет бороться с помехами, возникающими в должным образом спроектированной квантовой системе во время процесса обработки квантовой информации. Значительный прогресс был достигнут в обобщении данных идей (Knill and Laflamme 1997, Ekert and Macchiavello 1996, Bennett et. al. 1996b, Gottesman 1996, Calderbank et. al. 1997). Существенное улучшение метода было продемонстрировано Шором и Китаевым (1996). Они показали, что исправление ошибки происходит даже тогда, когда сами операции коррекции являются неидеальными. Такие методы приво-

дят к появлению понятия «исправление ошибок в процессе вычисления», объяснение которого дано Прескилом (Preskill, 1997).

Если, что кажется почти очевидным, квантовые вычисления осуществимы только при условии исправления квантовых ошибок, то связь между квантовой теорией информации и квантовыми компьютерами может оказаться более тесной, чем между теорией информации Шеннона и классическими компьютерами. Сам по себе метод исправления ошибок не обеспечивает точного квантового вычисления, поскольку не защищает от всех видов помех. Однако тот факт, что этот метод вообще возможен является очень важным.

Существующий только на бумаге компьютер не способен выполнить какие-либо практические вычисления. В конце концов, разрешить спорный вопрос, существующий в квантовой информатике относительно осуществимости построения квантового компьютера, может быть решен лишь путем создания самого квантового компьютера. К настоящему времени несколькими авторами были предложены его схемы, опирающиеся на идеи Дойча, но более полно проработанные в физическом плане (Teich et. al. 1988, Lloyd 1993, Berman et. al. 1994, DiVincenco 1995b). Перспективной является задача нахождения достаточно сложной системы, чья эволюция являлась бы одновременно когерентной (т.е. унитарной) и контролируемой. Недостаточно, чтобы система была лишь частично квантово-механической, как в твердотельных «квантовых точках» («quantum dots»), либо чтобы существовали неявные предположения относительно недостижимых точности или охлаждения, что часто предполагается в случае с твердотельными устройствами. Кирак (Cirac) и Золлер (Zoller) в 1995 г. предложили использовать линейную ионную ловушку, что является значительным шагом на пути создания компьютера, поскольку трудами людей, занимающихся вопросами ионной ловушки, уже достигнуты экспериментально необходимая точность и низкая температура. Особенно следует отметить достижения группы под руководством Уинленда (Winland), которая продемонстрировала в том же году охлаждение ионной ловушки до основного состояния (Diedrich et. al. 1989, Monroe et. al. 1995). Совсем недавно Gershenfeld and Chuang (1997) и Cory et. al. (1996, 1997) показали, что требования квантовых вычислений могут быть удовлетворены с помощью метода ядерного магнитного резонанса (ЯМР). Данный метод также является многообещающим. Могут использоваться и методы, предложенные Привма-

ном (Privman et. al. 1997), Лоссом (Loss) и ДиВинченцо (DiVincenzo, 1997).

На сегодняшний день еще не создан ни один квантовый компьютер и, скорее всего, он не будет создан при жизни автора, если рассматривать его с точки зрения алгоритма Шора и требовать от него разложения на множители больших чисел. Однако, если вместо вышеуказанного требуется устройство для проверки идей квантовой теории информации, то для этих целей необходимо лишь несколько квантовых битов. Такое устройство может быть создано в ближайшем будущем. Простые двухбитовые операции были осуществлены в различных физических экспериментах: например, в эксперименте с использованием метода магнитного резонанса, а операции над 3–10 кубитами сейчас являются вполне осуществимыми. В связи с вышеуказанным можно отметить следующие эксперименты: Brune et. al. (1994), Monroe et. al. (1995), Turchette et. al. (1995) и Mattle et. al. (1996).

Глава 2
Классическая теория информации

В этой и последующей главах будет рассмотрена классическая теория информации и вычислений. Материал этих глав является учебным (Minsky, 1967, Hamming, 1986), но он вошел в эту книгу, поскольку служит основой для квантовой теории информации и вычислений и может быть полезен физикам, для которых нижеизложенные идеи могут оказаться неизвестными.

2.1. Меры (количества) информации

Основной задачей классической теории информации является задача определения меры или, другими словами, количества информации. Предположим, вы узнаете значение числа X. Сколько при этом вы получаете информации? Ответ зависит от того, что вы уже знали относительно X. Например, если вам заранее известно, что X равно 2, то вы не узнаете ничего нового, т. е. не получите информации. С другой стороны, если вам заранее известно, что значение X определяется броском игральной кости, то здесь получение значения числа соответствует увеличению информации. В этом состоит основное парадоксальное свойство, заключающееся в том, что информация часто является мерой незнания: информационное содержание (или «собственная информация») величины X определяется как информация, которая может быть получена при определении значения данной величины X.

Если X является случайной величиной и принимает значение x с вероятностью $p(x)$, то информационное содержание переменной X определяется как

$$S(\{p(x)\}) = -\sum_x p(x)\log_2 p(x). \qquad (1)$$

Следует отметить, что логарифм берется по основанию 2, а величина S всегда положительна, поскольку вероятность появления значения x подчиняется условию $p(x) \leqslant 1$. Здесь зависимость (1) является функцией распределения вероятностей значений переменной X.

Это необходимо запомнить, поскольку в дальнейшем вместо выражения $S(\{p(x)\})$ будет использоваться выражение $S(X)$. Очевидно, что выражение $S(X)$ означает не функцию от X, а информационное содержание переменной X. Иногда, по понятным причинам, выражение $S(X)$ называют энтропией.

Если изначально известно, что $X = 2$, то $p(2) = 1$, другие слагаемые под знаком суммы отсутствуют. Это приводит к тому, что $S = 0$ и величина X, таким образом, не обладает информационным содержанием. Если, с другой стороны, значение величины X определяется броском игральной кости, то $p(x) = \frac{1}{6}$ для $x \in \{1, 2, 3, 4, 5, 6\}$. Таким образом, $S = -\log_2 \frac{1}{6} \simeq 2{,}58$. Если величина X может принимать N различных значений, то ее информационное содержание (или энтропия) имеет максимальное значение для плоской функции распределения вероятностей p, где $p(x) = \frac{1}{N}$ (для обыкновенной кости величина $S \simeq 2{,}58$, а в случае с утяжеленной с одной стороны кости, для которой $p(6) = \frac{1}{2}$, $p(1, \ldots, 5) = \frac{1}{10}$, величина $S \simeq 2{,}16$). Это согласуется с тем фактом, что объем информации (которую можно получить при определении значения X) наибольший, когда предварительные знания о величине X минимальны.

Таким образом, максимальный объем информации, который в принципе может содержаться в переменной, способной принимать N разных значений, равен $\log_2(N)$. Логарифм берется по основанию 2 по соглашению. Этот выбор определяет единицу информации: $S(X) = 1$, если величина X принимает два значения с равными вероятностями. Таким образом, двоичная переменная или переменная, принимающая два значения, содержит единицу информации. Эта единица называется битом. Как правило, значения бита записывается в виде двоичных чисел: 0 и 1.

В случае с двоичной переменной можно определить вероятность появления величины $X = 1$ как p, тогда вероятность появления величины $X = 0$ равна $1 - p$. Сама информация может быть выражена как функция только от вероятности p:

$$H(p) = -p \log_2 p - (1 - p) \log_2 (1 - p). \qquad (2)$$

Функция $H(p)$ называется энтропийной и ее область значений равна $0 \leqslant H(p) \leqslant 1$.

В последующем значение основания логарифма будет опущено, т. е. будет предполагаться, что все логарифмы берутся по основанию 2, если другое не оговорено.

Вероятность того, что величина $Y = y$ при условии, что величина $X = x$ записывается как $p(y|x)$. Условная энтропия $S(Y|X)$ определяется как

$$S(Y|X) = -\sum_x p(x) \sum_y p(y|x) \log p(y|x) = \tag{3}$$

$$= -\sum_x \sum_y p(x, y) \log p(y|x), \tag{4}$$

где уравнение (4) выводится с помощью выражения $p(x, y) = p(x)p(y|x)$ ($p(x, y)$ определяет вероятность появления величины $X = x$ и $Y = y$). Обращаясь к определению, можно сказать, что величина $S(Y|X)$ является мерой усредненного количества информации, содержащегося в величине Y, если известно значение величины X. Заметим, что неравенство $S(Y|X) \leqslant S(Y)$ выполняется всегда, а неравенство $S(Y|X) \neq S(X|Y)$ — в большинстве случаев.

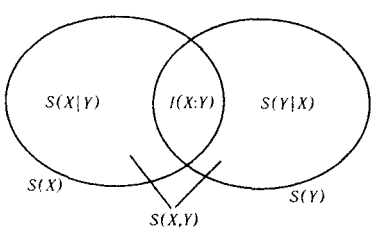

Рис. 3. Зависимость между мерами классической информации

Понятие условной энтропии главным образом необходимо для перехода к следующей величине: полному количеству информации (mutual information), определяемому как:

$$I(X : Y) = \sum_x \sum_y p(x, y) \log \frac{p(x, y)}{p(x)p(y)} = \tag{5}$$

$$= S(X) - S(X|Y). \tag{6}$$

По определению, величина $I(X : Y)$ есть мера количества информации, содержащейся в величинах X и Y друг относительно друга[1]. Если величины X и Y являются независимыми, то $p(x, y) = p(x)p(y)$ и, следовательно, величина $I(X : Y) = 0$. Зависимости между основными

[1]Многие авторы используют выражение $I(X;Y)$ вместо $I(X : Y)$. Однако здесь используется последний вариант, поскольку знак «:» отражает тот факт, что $I(X : Y) = I(Y : Z)$.

мерами информации показаны на рис. 3. Читателю в качестве упражнения предлагается доказать, что величина $S(X, Y)$, определяющая количество информации о величинах X и Y (т.е. это информация, которую можно получить при определении как X, так и Y, если первоначально их значение неизвестно), удовлетворяет уравнению $S(X, Y) = S(X) + S(Y) - I(X : Y)$.

Информация может исчезать, но не может самопроизвольно возникнуть из ниоткуда. Это важное замечание нашло математическое отражение в *неравенстве обработки данных*:

$$\text{если} \quad X \to Y \to Z, \quad \text{то} \quad I(X : Z) \leqslant I(X : Y). \tag{7}$$

Выражение $X \to Y \to Z$ означает, что величины X, Y и Z образуют последовательность (марковскую цепь), где Z зависит от Y, но не зависит напрямую от X, т.е. $p(x, y, z) = p(x)p(y|x)p(z|y)$. Смысл данного неравенства заключается в том, что величина Y (информационный процессор) передает величине Z не больше информации о X, чем сама получает.

2.2. Сжатие информации

Предварительно определив объем информации согласно уравнению (1), необходимо доказать, что он действительно является удобной мерой информации. С первого взгляда даже подход к этой задаче не является очевидным. Один из основных вкладов классической теории информации заключается в обеспечении подходящих методов рассмотрения информации. Для описания данных методов рассмотрим простую ситуацию: предположим, что некто (традиционно это Алиса) знает значение величины X и желает сообщить его Бобу. Здесь можно ограничиться простейшим случаем, когда величина X принимает лишь два возможных значения: «да» либо «нет». Будем говорить, что Алиса является «источником» с «алфавитом» из двух символов. Алиса общается с Бобом с помощью двоичных цифр (нули и единицы). Будем определять объем информации, содержащейся в величине X, посредством определения среднего количества битов, которые Алиса должна передать Бобу для того, чтобы он узнал значение X. Очевидно, она должна передать значение 0, если величина X принимает значение «да», и 1 — если принимает значение «нет». Таким образом, для каждого переданного значения X объем информации равен одному биту.

Однако, что произойдет, если определить величину X как случайную, но с большей вероятностью принимающую значение «нет», чем «да»? (В качестве примера подойдут решения, исходящие от субсидирующей организации.) В этом случае более эффективная передача может быть обеспечена, если Алиса будет придерживаться следующих действий.

Пусть p обозначает вероятность того, что величина X равна 1, а $1-p$ — вероятность того, что $X=0$. Алиса должна ждать, пока для сообщения не наберется n значений величины X, причем n должно быть достаточно большим. Среднее число единиц последовательности из n значений равно np, и, следовательно, число единиц в любой заданной последовательности близко к этому значению. Предположим, что величина np является целым числом. Тогда вероятность появления последовательности, содержащей np единиц, равна:

$$p^{np}(1-p)^{n-np} = 2^{-nH(p)}. \tag{8}$$

Читатель может убедиться, что обе части данного выражения действительно равны между собой, причем в правой части неявно указывается путь обобщения аргумента. Такая *последовательность* называется *типичной*. Говоря более точно, все члены множества последовательностей удовлетворяют неравенству

$$2^{-n(H(p)+\varepsilon)} \leqslant p(\text{последовательность}) \leqslant 2^{-n(H(p)-\varepsilon)}. \tag{9}$$

Здесь можно показать, что n значений, собранных Алисой, образуют типичную последовательность с вероятностью, большей, чем $1-\varepsilon$ при достаточно больших значениях n вне зависимости от того, несколько мало ε. Это значит, что Алисе не нужно отправлять Бобу n битов для того, чтобы он узнал n значений величины. Она должна лишь сообщить ему, какую *типичную последовательность* она имеет. Предварительно они должны договориться об обозначении типичных последовательностей: например, они могут договориться нумеровать их в порядке возрастания двоичной величины (двоичного значения). Алисе нужно передать не всю последовательность, а только ее обозначение. Чтобы понять, насколько эффективен данный метод общения, достаточно показать, что вероятности появления типичных последовательностей, количество которых составляет $2^{nH(p)}$, равны. Очевидно, что для передачи одной из $2^{nH(p)}$ последовательностей Алисе необходимо отправить $nH(p)$ битов. Более того, Алиса не сможет сделать общение

более эффективным (т. е. передавать меньшее число битов), поскольку события, связанные с появлением типичных последовательностей, равновероятны: дальнейшее оперирование информацией не будет продуктивным. Таким образом, объем информации, содержащийся в каждом значении величины X первоначальной последовательности, равен $H(p)$, что соответствует уравнению (1).

Математические подробности, появившиеся в вышеуказанных рассуждениях, вытекают из закона больших чисел, который гласит, что при малых ε, δ и для достаточно больших n выполняется неравенство

$$p(|m - np| < n\varepsilon) > 1 - \delta, \tag{10}$$

где m — число единиц, содержащееся в последовательности n значений. При больших n число единиц m будет отлично от их среднего количества np на величину, как угодно малую по сравнению с n. Например, в данном случае распределение нулей и единиц соответствует биномиальному:

$$p(n, m) = C(n, m)p^m(1-p)^{n-m} \simeq \tag{11}$$

$$\simeq \frac{1}{\sigma\sqrt{2\pi}} e^{-(m-np)^2/2\sigma^2}, \tag{12}$$

где нормальное (гауссово) распределение получено для $n, np \to \infty$, среднеквадратичного отклонения $\sigma = \sqrt{np(1-p)}$ и $C(n,m) = \dfrac{n!}{(m!(n-m)!)}$.

Вышеупомянутые рассуждения приводят к практически важному результату, связанному с уравнением (1): для передачи n значений величины X необходимо переслать по каналу связи $nS(X) \leqslant n$ битов. Такой метод называется *сжатием информации*, а сама идея подобной связи называется теоремой бесшумного кодирования Шэннона.

Идея типичных последовательностей привела к появлению способов изменения объема информации, но сам метод сжатия информации не является лучшим, поскольку Алисе необходимо накопить большое количество значений величины, перед тем как передать Бобу какую-либо информацию. Более удачный способ связи заключается в накоплении Алисой нескольких значений, например, четырех, и передаче их как одного «сообщения» наиболее удобным методом. Хаффман установил оптимальный метод, согласно которому Алиса использует короткие наборы битов для передачи наиболее вероятных «сообщений» и более

Сообщение	Хаффман	Хемминг
0000	10	0000000
0001	000	1010101
0010	001	0110011
0011	11000	1100110
0100	010	0001111
0101	11001	1011010
0110	11010	0111100
0111	1111000	1101001
1000	011	1111111
1001	11011	0101010
1010	11100	1001100
1011	111111	0011001
1100	11101	1110000
1101	111110	0100101
1110	111101	1000011
1111	1111001	0010110

Таблица 1. Коды Хаффмана и Хемминга. В левом столбце представлены шестнадцать возможных четырехбитовых сообщений, в двух оставшихся столбцах показаны закодированные варианты сообщений. Код Хаффмана соответствует сжатию информации: содержащие наименьшее количество битов коды соответствуют наиболее вероятным сообщениям. Код соответствует случаю, когда вероятность появления нуля в сообщении в три раза больше вероятности появления единицы. Код Хаффмана является кодом, исправляющим ошибки: каждое кодовое слово отличается от любого другого по крайней мере в трех местах. Таким образом, возможно исправление одной ошибки. Кроме того, код Хемминга является линейным: все слова являются линейными комбинациями чисел 1010101, 0110011, 0001111, 1111111

длинные наборы для передачи менее вероятных сообщений (см. таблицу 1). Процесс трансляции состоит из «кодирования» и «декодирования» (см. рис. 4). Такая терминология не вызывает никакого желания держать информацию в тайне.

Согласно теореме бесшумного кодирования Шеннона, при вероятности p, равной $\frac{1}{4}$, с использованием лучшей методики сжатия информации необходимо в среднем $4H\frac{1}{4} \simeq 3{,}245$ битов для передачи сообщения, состоящего из четырех значений величины X. В коде Хаффмана, приведенном в таблице 1, используется в среднем 3,273 бита. Это число,

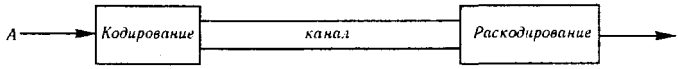

Рис. 4. Стандартный канал связи («герб информационного террориста»). Источник (Алиса) формирует информацию, оперирует ею («кодирует») и пересылает по каналу. На приемнике (Боб) происходит «дешифрация» полученных значений и извлечение информации

близкое к минимально возможному, указывает на большу́ю эффективность методов, подобных методу Хаффмана.

Сжатие информации — это понятие, имеющее огромное практическое значение. Оно используется в телесвязи, например, при сжатии информации, необходимой для передачи изображения в память компьютера. Сжатие информации, с точки зрения проектирования каналов связи, является уникальным инструментом. Предположим, что имеется телефонная линия в гористой местности, однако ее пропускная способность недостаточна, скажем, для передачи активного видео изображения. Типичное инженерное решение заключается в замене линии другой, имеющей более высокую скорость передачи. Однако вместо этого теория информации предлагает использовать ту же линию, но для передачи обработанной информации (подвергнутой сжатию и декомпрессии на разных концах линии). Довольно неожиданно то, что пригодность кабеля зависит не только от него самого, но и от способа обработки передаваемой информации.

2.3. Двоичный симметричный канал

До настоящего момента рассматривались лишь случаи связи по идеальному каналу, т. е. по каналу без помех (noise-free channel). Также были получены важные результаты, имеющие практическое значение: найдена мера максимально возможного сжатия информации (теорема бесшумного кодирования Шеннона) и практический метод сжатия информации (кодирование Хаффмана). Теперь необходимо рассмотреть другой важный вопрос: связь с помехами. Как и в предыдущем разделе, будет рассмотрен простейший пример с целью проиллюстрировать общие принципы.

Предположим, что имеется двоичный канал, т. е. такой канал, по которому Алиса может передавать Бобу нули и единицы. При исполь-

зовании канала без помех нулю или единице на выходе соответствуют ноль или единица на входе ($0 \to 0$ и $1 \to 1$). Однако, в случае канала с помехами, единица может стать нулем, и наоборот. Существует множество типов помех. Например, вероятность ошибочного «переброса бита» из значения 0 в значение 1 ($0 \to 1$) должна совпадать с вероятностью «переброса бита» $1 \to 0$. В противном случае, канал будет обладать свойством «релаксации» по отношению к 0, т. е. переброс $1 \to 0$ будет иметь место, а переброс $0 \to 1$ нет. Кроме того, подобные ошибки могут возникать независимо друг от друга от бита к биту либо внезапно. Помехи, независимо влияющие на различные биты и вызывающие как переброс $0 \to 1$, так и переброс $1 \to 0$, являются наиболее важными, поскольку искажают важные свойства многих процессов, встречающихся в реальных ситуациях. В случае, когда ошибки $0 \to 1$ и $1 \to 0$ равновероятны, то канал с помехами называется двоичным симметричным каналом. Данный канал имеет лишь один показатель p, определяющий вероятность ошибки, приходящейся на каждый передаваемый бит. Пусть сообщение, передаваемое Алисой по каналу, есть X, а сообщение с помехами, принимаемое Бобом, есть Y. Таким образом, Боб сталкивается с задачей наиболее точного выделения сообщения X из сообщения Y. Если сообщение X состоит из бита, то Бобу придется воспользоваться следующими условными вероятностями:

$$p(x = 0|y = 0) = p(x = 1|y = 1) = 1 - p,$$
$$p(x = 0|y = 1) = p(x = 1|y = 0) = p,$$

которые, согласно уравнениям (2) и (3), дают: $S(X|Y) = H(p)$. Таким образом, из уравнения (6), определяющего полную информацию, получаем:

$$I(X : Y) = S(X) - H(p). \tag{13}$$

Очевидно, наличие в канале помех ограничивает информацию о сообщении Алисы X, находящуюся в принятом Бобом сообщении Y. Кроме того, согласно неравенству (7) относительно обработки информации, Боб не может, оперируя сообщением Y, увеличить объем информации о сообщении X. Однако уравнение (13) показывает, что связь между Алисой и Бобом станет лучше при больших значениях $S(X)$. Общий вывод заключается в том, что качество передаваемой информации зависит как от ее источника, так и от свойств канала. Полезно отдельно

определить свойства канала для того, чтобы узнать его способность передавать информацию. Одним из изменяемых свойств является пропускная способность (емкость) канала и определяется как максимально возможное полное количество информации $I(X:Y)$ между входом и выходом, максимизированное по всем возможным источникам:

$$\text{емкость канала } C \equiv \max_{\{p(x)\}} I(X:Y). \tag{14}$$

Емкость канала определяется отношением числа битов на выходе к одному символу на входе и ее значение для двоичных каналов должно находится между нулем и единицей.

Несмотря на данное определение, уравнение (14) не позволяет относительно просто сравнивать каналы, поскольку требует максимизации по входным стратегиям, которые нетривиальны. Задача определения емкости $C(p)$ двоичного симметричного канала является основной в теории информации, однако ее решение достаточно простое. Из уравнений (13) и (14) видно, что его можно представить в виде:

$$C(p) = 1 - H(P). \tag{15}$$

Это условие получается при $S(X) = 1$ (т.е. $p(x=0) = p(x=1) = \frac{1}{2}$).

2.4. Коды, исправляющие ошибки

До настоящего момента рассматривался лишь вопрос о том, сколько информации проходит через канал с помехами и какое ее количество теряется. Объем посылаемой Алисой Бобу информации ограничен величиной $C(p)$ на каждый передаваемый символ. Однако предположим, что Боб обезвреживает бомбу, а Алиса стоит в отдалении и кричит ему о том, какой провод необходимо перерезать. Она не может надеяться на то, что Боб поймет ее правильно, если произнесет фразу: «режь синий провод» лишь один раз. Алиса будет повторять эту фразу несколько раз, а Боб будет ждать до тех пор, пока не будет уверен, что правильно ее понял. Связь без ошибок может быть достигнута даже при использовании канала с помехами. В данном примере показано, что можно снизить долю ошибок путем увеличения количества передаваемой информации. Следующий шаг в данном курсе по изучению теории информации заключается в определении более мощных методов борьбы с помехами (Hamming 1986; Hill 1986, Jones 1979; MacWilliams and Sloane 1977).

В дальнейшем понадобятся следующие понятия. Множество $\{0, 1\}$ определяется как группа (поле Галуа $GF(2)$), в которой операции $+$, $-$, $\times$, $\div$ выполняются по модулю 2 (таким образом, $1 + 1 = 0$). Двоичное слово, состоящее их n битов представляется вектором, имеющим n компонент, например слово 001 может быть представлено вектором (0, 0, 1). Множество подобных векторов образуют аддитивно замкнутое векторное пространство (образуют векторное пространство по сложению), т. к., например, сумма двух слов: 011+101 в векторной форме и по правилам векторного сложения равна 110, поскольку $(0, 1, 1) + (1, 0, 1) = (0 + 1, 1 + 0, 1 + 1) = (1, 1, 0)$. Это действие эквивалентно операции «исключающее ИЛИ» (XOR), выполняемой поразрядно между двумя двоичными словами.

Воздействие помехи на слово u может быть выражено следующим образом: $u \to u' = u + e$, где e обозначает вектор ошибки, который указывает на положение переброшенного вследствие помехи бита. Например, переброс битов в слове $u = 1001101 \to u' = 1101110$ может быть выражен как $u' = u + 0100011$. Код C, исправляющий ошибку, представляет множество слов таких, что

$$u + e \neq v + f \quad \forall u, v \in C (u \neq v) \; \forall e, f \in E, \tag{16}$$

где E — множество векторов ошибок, которые можно исправить посредством кода C, включая «нулевой вектор ошибки» $e = 0$ (соответствует случаю отсутствия ошибки). Для использования такого кода Алисе и Бобу нужно договориться о том, какому сообщению соответствует то или иное кодовое слово u. После этого Алиса будет передавать по каналу только кодовые слова. Поскольку в канале присутствуют помехи, Боб будет вместо слова u принимать слово $u + e$. Однако Боб сможет однозначно выделить из слова $u + e$ слово u, поскольку, согласно условию (16), он не сможет принять слово $u + e$, если Алиса будет передавать какое-либо другое кодовое слово v.

Пример кода, исправляющего ошибки, представлен в правом столбце таблицы 1. Этот код в честь его автора называется кодом Хэмминга [7, 4, 3]. Добавление $[n, k, d]$ означает, что всего имеется 2^k кодовых слов, каждое слово состоит из n битов и все слова отличаются друг от друга значениями по крайней мере d битов. Из последнего свойства следует, что условие (16) выполняется для любой ошибки, изменяющей не более одного бита. Другими словами, множество E исправляемых ошибок определяется как {0000000, 1000000, 0100000, 0010000, 0001000,

0000100, 0000010, 0000001}. Следует отметить, что максимальное количество членов множества E равно 2^{n-k}. Отношение $\frac{k}{n}$ называется *коэффициентом кода* (rate of the code), поскольку каждый передаваемый блок из n битов содержит k битов информации или, другими словами, $\frac{k}{n}$ битов информации приходятся на каждый передаваемый бит.

Величина d называется «минимальным расстоянием» кода и имеет важное значение при кодировании, когда помехи, как, например, в двоичном симметричном канале, воздействуют независимо на каждый бит. Код с минимальным расстоянием, равным d, исправляет все ошибки, появившиеся не более чем в $\frac{d}{2}$ битах передаваемого кодового слова. Кроме того, в случае с независимыми помехами данное количество ошибок наиболее вероятно. Фактически, вероятность того, что в слове u из n битов возникнет m ошибок, определяется биномиальным распределением (11). Поэтому, если код исправляет число ошибок больше среднего их количества np, то существует высокая вероятность того, что в целом работа кода будет успешной.

Главным выводом классической теории информации является то, что мощные коды, исправляющие ошибки, существуют.

Теорема Шеннона. *Если коэффициент кода $\frac{k}{n} < C(p)$, а число битов n достаточно большое, то существует двоичный код для передачи информации со сколь угодно малой вероятностью ошибки.*

Здесь вероятность ошибки означает вероятность появления неисправляемой ошибки, которая приводит к неправильному истолкованию Бобом принятого слова. Из теоремы Шеннона следует, что вместо решения сложной и дорогой задачи создания каналов связи с низким уровнем помех, можно снизить уровень помех посредством кодов, исправляющих ошибки, другими словами, посредством обработки информации. Следствия из теоремы Шеннона показаны на рис. 5.

Распознавание кодов с большими значениями коэффициента $\frac{k}{n}$ и расстояния d является основной задачей теории кодирования. Поскольку два данных условия несовместимы, то между ними требуется найти какой-либо компромисс. Данная задача действительно очень сложна и не имеет общего решения. Для того чтобы связать вышеизложенное с кодами, исправляющими ошибки, необходимо напомнить одно очень важное понятие, а именно, понятие матрицы с контролем по четности

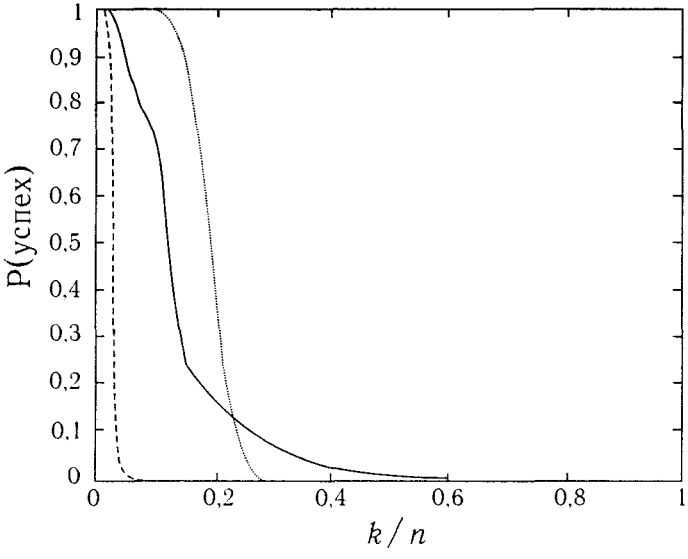

Рис. 5. Иллюстрация к теореме Шеннона. Алиса с целью передать Бобу k битов информации пересылает по каналу с помехами $n = 100$ битов. На рисунке показана зависимость вероятности правильного интерпретирования Бобом полученной информации от отношения k/n при вероятности ошибки на бит: $p = 0{,}25$. Емкость канала $C = 1 - H(0{,}25) \approx 0{,}19$. Штриховая линия: каждый передаваемый Алисой бит повторяется n/k раз. Сплошная линия: Алиса использует наилучший вариант линейного кода, исправляющего ошибки с коэффициентом k/n. Точечная линия определяет эффективность кодов, исправляющих ошибки при увеличении n и наглядно иллюстрирует теорему Шеннона

(parity-cheek matrix). Код, исправляющий ошибки, называется линейным, если он является замкнутым по сложению, т. е. $u + v \in C$ для любых u, $v, \in C$. Подобный код полностью определяется его матрицей с контролем по четности H, которая является множеством $(n - k)$ линейно независимых n-битовых слов, удовлетворяющих условию: $H \cdot u = 0$ для любого $u \in C$.

Отметим следующее важное свойство матрицы

$$H \cdot (u + e) = (H \cdot u) + (H \cdot e) = H \cdot e. \qquad (17)$$

Из этого свойства следует, что если Боб будет определять значение $H \cdot u'$

для искаженного помехами принятого слова $u' = u + e$, то в результате он получит $H \cdot e$ вне зависимости от того, какое слово u передала ему Алиса. Если данное вычисление будет выполняться автоматически, то Боб сможет узнать значение $H \cdot e$, называемое *синдромом ошибки* без определения слова u! Если Боб сможет из величины $H \cdot e$ выделить значение ошибки e (можно показать, что это возможно для всех исправляемых кодов), то он сумеет исправить сообщение, удаляя из него ошибку e, даже не вникая в его смысл! При исправлении квантовых ошибок данное действие является основным объяснением тому, как можно исправить квантовое состояние не нарушая его.

Глава 3
Классическая теория вычислений

Теперь обратимся к теории вычислений. Главным образом, она затрагивает такие вопросы, как «Что является определением вычислимости?», «Какие средства необходимы для вычисления?».

Фундаментальными средствами, необходимыми для вычисления, являются средствами хранения и обработки символов. Существенными вопросами являются такие, как: «Насколько сложными должны быть символы и операции над ними?», «Сколько символов и операций необходимо для вычисления?».

Основной вывод теории заключатся в том, что вычисление считается сложным или неэффективным, если объем необходимых для него средств возрастает экспоненциально в зависимости от размера задачи, которую необходимо решить. Размер задачи задается количеством информации, необходимой для ее описания. На базовом уровне из вышесказанного следует, что вычислительное устройство должно уметь оперировать не только унарными[1], но и двоичными символами. В противном случае число ячеек памяти будет экспоненциально зависеть от количества информации, которую необходимо обработать. С другой стороны, нет необходимости использовать десятичную систему счисления (10 символов) или любую другую систему, «алфавит» которой состоит более чем из двух символов, что существенно упрощает структуру компьютера и операции им выполняемые.

При работе с n двоичными символами нет необходимости оперировать сразу всеми символами. Можно показать, что любое преобразование может осуществляться при обработке одного или пары символов за раз. Двоичный «логический гейт» имеет на входе два бита x, y и вычисляет функцию $f(x, y)$. Поскольку функция может принимать значения 0 и 1, и существует четыре возможных варианта входных данных, то можно определить 16 возможных видов функции f. Множество,

[1] В унарном обозначении используется лишь символ 1. Положительные целые числа будут записываться следующим образом: 1, 11, 111, 1111 ...

состоящее из 16 различных логических гейтов, образует так называемое «универсальное множество», поскольку, комбинируя такие гейты в последовательности, можно осуществить любое преобразование n битов. Более того, действие некоторых гейтов может быть воспроизведено посредством комбинирования других гейтов. Таким образом, не нужно использовать все 16 функций, фактически потребуется лишь один гейт: И-НЕ (NAND gate) (на выходе этого гейта появится 0, только если оба входных значения равны 1).

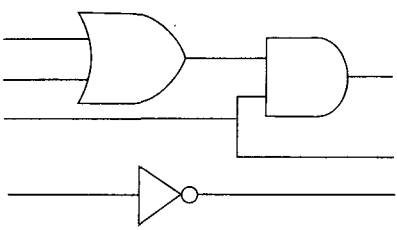

Рис. 6. Классический компьютер может быть построен на основе сети логических гейтов

Путем объединения логических гейтов можно обрабатывать символы, состоящие из n битов (см. рис. 6). Данный подход называется сетевой моделью вычисления. Он полезен в том смысле, что от него можно перейти к модели квантового вычисления, которая на сегодняшний день находит широкое применение в экспериментах. Основными составляющими данной модели являются множество битов, многократно повторяющийся универсальный логический гейт и связи между гейтами.

3.1. Универсальный компьютер. Машина Тьюринга

Слово «универсальный» по отношению к компьютерам приобретает более глубокий смысл. Тьюринг показал, что возможно создать *универсальный* компьютер, имитирующий работу любого другого вычислительного устройства следующим образом: пусть машина Тьюринга T обрабатывает входное значение x, поступающее с входной ленты, и имеет на выходе значение $T(x)$ (рис. 7). Полностью определить машину Тьюринга можно посредством зависимости выходных значений от 0 и 1 на входной ленте для всех ее возможных внутренних конфигураций, число которых конечно. Само по себе это определение может быть представлено в виде двоичного числа $d[T]$. Тьюринг показал, что существует машина U, называемая универсальной машиной Тьюринга, которая обладает следующими свойствами:

$$U(d[T], x) = T(x), \tag{18}$$

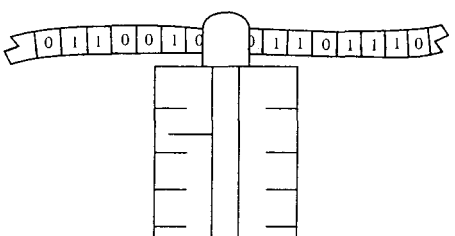

Рис. 7. Машина Тьюринга. Представляет собой умозрительное механическое устройство. Можно показать, что оно может эффективно имитировать все классические методы вычислений. Машина содержит конечное множество внутренних состояний и обладает жесткой схемой. За определенный момент времени машина считывает с ленты один двоичный символ. Ответное действие (реакция) машины зависит только от данного символа s и от внутреннего состояния G и заключается в записи символа s' на место считываемого символа s, перехода в новое состояние G' и сдвиге ленты на одну позицию в направлении d (влево или вправо). Таким образом, внутренняя структура машины может определяться конечным списком установленных правил вида $(s,\ G \to s',\ G',\ d)$. Особым внутренним состоянием является состояние «останов»; перейдя в него машина прекращает работу. Исходная «программа» с ленты преобразуется машиной в выходные данные, которые отображаются на данной ленте

а число шагов, необходимых машине U для имитации каждого шага машины T, является полиномиальной (а не экспоненциальной) функцией от длины (количества знаков) $d[T]$. Другими словами, если лента входных данных машины U содержит как описание машины T, так и входные значения x, то машина U сможет вычислить без экспоненциального увеличения времени обработки значения функции таким же образом, что и машина T (какова бы ни была сама машина T).

В заключение можно показать, что другие модели вычислений (например, сетевая модель) являются эквивалентными по вычислениям машине Тьюринга: они позволят работать с теми же функциями, с той же производительностью вычислений (см. следующий раздел). Таким образом, в концепции универсальной машины показано, что определенная конечная степень сложности устройства достаточна для обеспечения самой общей обработки информации. Это положение является фундаментальным выводом в информатике. Действительно, мощность ма-

шины Тьюринга и ей подобных машин настолько велика, что Church (1936) и Turing (1936) определили «тезис Чёрча–Тьюринга», который гласит, что:

Любая функция, к которой подходит определение «вычислимая», может быть обработана на универсальной машине Тьюринга.

Этот тезис не доказан. Однако он уже выдержал несколько попыток найти пример, его опровергающий, что само по себе имеет большое значение. Благодаря этому тезису современный компьютер общего назначения решает самые разносторонние задачи — поскольку «вычислимые функции» включают в себя такие задачи, как обработка слов, контроль на производстве и т. д. Квантовый компьютер, о котором говорится в разделе 6, позволяет по-новому взглянуть на этот основной тезис.

3.2. Сложность вычисления

Описав идеи универсального компьютера, можно классифицировать задачи, связанные с вычислениями по их сложности, следующим образом: считается, что данный алгоритм должен быть направлен на решение не частной задачи (например, вычислить квадрат числа 237), а на решение класса задач (например, при данном x вычислить его квадрат); количество информации, передаваемой компьютеру для определения задачи, равно $\log x$, т. е. равно количеству битов, необходимых для хранения значения x. *Сложность вычислений* для какой-либо задачи определяется как число шагов s, которые необходимы машине Тьюринга для завершения какого бы то ни было алгоритма по решению данной задачи. Для сетевой модели сложность вычисления определяется числом требуемых логических гейтов. Если существует алгоритм, для которого число шагов s полиномиально зависит от объема информации L (например, $s \propto L^3 + L$), то считается, что соответствующая этому алгоритму задача поддается обработке и ее относят к классу сложности «P». Если же число шагов s возрастает экспоненциально по мере увеличения информации L (например, $s \propto 2^L = x$), то задача считается сложной и она будет относиться к другому классу сложности. Очень часто бывает проще проверить решение, т. е. узнать, является ли оно верным, чем искать его. Класс сложности «NP» включает в себя

множество задач, решение которых может быть проверено за полиномиальное время. Очевидно, что $P \in NP$, однако существуют задачи, входящие в класс NP, но не входящие в класс P (т.е. $NP \neq P$). Удивительным является то, что последнее утверждение никогда не было доказано, поскольку сложно исключить возможность существования алгоритмов, которые еще не найдены. Однако важно отметить, что частичное совпадение этих классов не зависит от модели вычисления, т.е. от тех или иных физических принципов, на которых построен компьютер, поскольку машина Тьюринга способна имитировать любой другой компьютер не с экспоненциальным, а с полиномиальным замедлением.

Важным примером не поддающейся решению задачи является задача о разложении числа на множители: задавшись сложным (т.е. не являющимся простым) числом x, необходимо определить один из его множителей. Если x является четным либо кратным какому-либо небольшому числу, то его множитель найти легко. Важно отметить ситуацию, когда простые множители числа x являются большими числами. В этом случае простой метод решения задачи не известен. Наиболее известен метод «решета числового поля» (Menezes et. al. 1997). Он реализуется за число шагов s порядка $s \sim \exp(2L^{1/3}(\log L)^{2/3})$, где $L = \ln x$. При использовании существующих на сегодняшний день вычислительных сетей определение множителей числа, состоящего из 130 десятичных знаков (Crandall, 1977), т.е. $L \simeq 300$, потребует число шагов $s \sim 10^{18}$, эта задача решаема, но само решение требует некоторых временных затрат (при скорости работы, равной 10^{12} операций в секунду, требуется 42 дня). Однако, если увеличить объем информации L в два раза, а число шагов s, соответственно, поднять до $s \sim 10^{25}$, задача станет неразрешимой: при современном уровне развития вычислительной техники ее решение займет миллион лет либо для ее решения необходимо увеличить быстродействие компьютера в миллион раз. В этом важном примере показано, что задача, «сложная» с точки зрения вычисления, является практически не просто трудно решаемой, она является невычислимой.

Задача разложения на множители имеет большое практическое значение, поскольку лежит в основе широко распространенных криптографических систем, подобных системам Ривеста (Rivest), Шамира (Shamir) и Адлемана (1979) (см. Hellman, 1979). Поскольку, задавшись сообщением M (в виде большого двоичного числа), можно легко получить его зашифрованный вариант как: $E = M^s \bmod c$, где s и c — тща-

тельно подобранные большие целые числа, которые могут быть общедоступны. Для расшифровки сообщения получатель определяет значение величины: $E^t \bmod c$, совпадающее со значением M. Причем t легко находится с помощью s и множителей c (Schroeder, 1984). На практике величина $c = pq$ задается как произведение двух достаточно простых чисел p и q, известных только тому пользователю, который задает значение c. Поэтому до тех пор, пока кто-нибудь не сумеет разложить на множители число c, этот пользователь будет единственным, кто будет способен прочитать данное сообщение. Следует отметить, что в подобной системе нет необходимости в распространении шифров: «шифры» c, s, обеспечивающие кодировку, общедоступны.

3.3. Невычислимые функции

Существуют и более сложные задачи, которые невозможно решить с помощью компьютера. При необходимости решения некоторых задач можно «прожить» то время, пока будет выполняться алгоритм. Но что делать в том случае, когда алгоритма вообще не существует? Подобные задачи называются *невычислимыми*. Наиболее ярким и важным примером таких задач является задача об останове. Характерная черта как программистов, так и компьютеров заключается в том, что время от времени они в своих действиях начинают двигаться по замкнутому кругу. В качестве примера рассмотрим следующую информацию: «Пока $x > 2$ делить x на единицу» при начальном значении величины x больше двух. Даже без практической реализации этого алгоритма можно видеть, что он не имеет завершения. Более интересным с математической точки зрения является следующий алгоритм: «Пока x равно сумме двух простых чисел, добавлять к x число два. В противном случае печать x. Останов» при начальном значении $x = 8$. Очевидно, данный алгоритм выполним, поскольку две пары простых чисел, меньших x, могут быть систематически найдены и сложены. Имеет ли данный алгоритм завершение? Если да, то он опровергает предположение Гольдбаха. С помощью подобных приемов обширный раздел математической и физической теории может быть сведен к вопросу: «Сможет ли тот или иной алгоритм завершиться после его запуска?» Если бы был известен какой-либо общий метод определения ответа на данный вопрос, то сам метод являлся бы очень мощным математическим инструментом. Очевидно, с его помощью можно было бы разрешить все вопросы математики.

Пусть существует возможность нахождения алгоритма общего вида, который определяет, сможет ли та или иная машина Тьюринга завершить свою работу при любых входных данных. Такой алгоритм дает ответ на следующий вопрос: «Даны значения x и $d[T]$. Сможет ли машина Тьюринга завершить работу, если на ее вход подать значение x?» Здесь $d[T]$ — описание машины T. Если такой алгоритм существует, то возможно определить такую машину Тьюринга T_H, которая будет завершать работу тогда и только тогда, когда машина $T(d[T])$ не сможет остановиться, где $d[T]$ — описание машины T. Здесь на входе машины T_H находится величина $d[T]$, которая содержит информацию как о машине Тьюринга T, так и о ее входных данных. Отсюда следует:

$$T_H(d[T]) \text{ имеет останов } \leftrightarrow T(d[T]) \text{ не имеет останова.} \qquad (19)$$

Но что произойдет, если в машину T_H направить описание ее самой $d[T_H]$? Тогда:

$$T_H(d[T_H]) \text{ имеет останов } \leftrightarrow T_H(d[T_H]) \text{ не имеет останова,} \qquad (20)$$

что является противоречивым. Посредством данных рассуждений Тьюринг показал, что не существует автоматических средств, которые определяют, сможет ли в общем случае машина Тьюринга завершить работу: таким образом, задача об останове является неразрешимой. Это значит, что математика и обработка информации, в общем случае, являются сложным организмом, состоящим из разнообразных идей, которые невозможно объединить в одном мощном алгоритме. Вышесказанное напрямую связано с теоремой Геделя.

Глава 4
Квантовая физика против физики классической

Для того чтобы перейти к квантовой теории информации, необходимо следующим образом определить принципы нерелятивистской квантовой механики (Shankar, 1980).

1. Состояние изолированной системы Q выражается посредством вектора $|\psi(t)\rangle$в гильбертовом пространстве.

2. Такие переменные, как положение и импульс называются наблюдаемыми величинами и представляются посредством эрмитовых операторов. Операторы положения и импульса X, P содержат в собственном базисе оператора X следующие матричные элементы:

$$\langle x|X|x'\rangle = x\delta(x-x'),$$
$$\langle x|P|x'\rangle = -i\hbar\delta'(x-x').$$

3. Вектор состояния подчиняется уравнению Шредингера

$$i\hbar\frac{d}{dt}|\psi(t)\rangle = H|\psi(t)\rangle, \tag{21}$$

где H — квантовый оператор Гамильтона (гамильтониан).

4. Постулат об измерениях.

Четвертый постулат, который не очевиден, является в какой-то степени спорным, поскольку совершенно различные объясняющие его подходы дают одни и те же прогнозы, а само понятие «измерение» в квантовой механике можно истолковать по-разному (Wheeler and Zurek 1983, Bell 1987, Reres 1993). Положение, справедливое для большинства практических случаев, заключается в том, что определенные физические взаимодействия являются распознаваемыми «измерениями», а их влияние на вектор состояния $|\psi\rangle$ состоит в изменении данного вектора на собственное состояние $|k\rangle$ измеряемой переменной. Причем выбор величины k является случайным, с вероятностью $P \propto |\langle k|\psi\rangle|^a$.

Переход $|\psi\rangle \rightarrow |k\rangle$ выражается посредством оператора проектирования $(|k\rangle\langle k|)/\langle k|\psi\rangle$.

Необходимо отметить, что в соответствии с вышеуказанными уравнениями эволюция изолированной квантовой системы всегда *единична.* Другими словами, вектор состояния может быть выражен как $|\psi(t)\rangle = U(t)|\psi(0)\rangle$, где $U(t) = \exp(-iH\,dt/\hbar)$ — унитарный оператор, $UU^{\dagger} = I$. Однако сложность заключается в том, что не существует абсолютно изолированной системы (т. е. такой системы, которая не взаимодействует с другими системами), кроме, возможно, всей Вселенной. Таким образом, в описании реальных систем всегда присутствует некоторое приближение, содержащееся в уравнении Шредингера.

Один из способов учета данных приближений — это описание как системы Q, так и той среды T, в которой она находится. Эволюция системы Q в первую очередь определяется уравнением Шредингера, но взаимодействие системы со средой T частично имеет характер измерения системы Q. Следствием этого взаимодействия является неединичная составляющая в эволюции системы Q, поскольку проекции уже не унитарны. Данное явление называется *потерей когерентности.* Все вышеуказанное потребуется для дальнейшего изложения.

Уже сейчас можно постепенно начать объединять физику и обработку информации, поскольку очевидно, что большинство природных процессов вокруг нас могут рассматриваться как формы обработки информации, а с другой стороны, современные компьютеры способны имитировать различные явления Природы. Здесь возникают очевидные, хотя и в некоторой степени неточные вопросы:

1. Может ли Природа по своей сути рассматриваться как информационный процессор? И можно ли из этого извлечь пользу?

2. Может ли компьютер имитировать все процессы Природы?

В соответствии с законами квантовой механики ответ на первый вопрос будет «да»[1], поскольку вектор состояния $|\psi\rangle$, занимающий центральное положение в квантовой механике, является понятием очень схожим с таким же понятием в науке об информации: данный вектор — это абстрактная величина, содержащая практически всю информацию

[1] Это совсем не означает, что подобное высказывание охватывает все, что можно сказать о Природе. Оно лишь является удобной абстракцией на описательном уровне физики. Я считаю, что физические «законы» недостаточны для, например, полного описания поведения человека, поскольку являются достаточно приближенными, что не оставляет людям места для свободы действий. (Polkinghorne 1994).

о системе Q. Определение «практически всю» является напоминанием не только о том, что вектор $|\psi\rangle$ полностью описывает систему Q, но и том, что данный вектор не содержит какую-либо постороннюю информацию, не связанную с системой Q. Значение вышесказанного для квантовой статистики газов Ферми и Бозе было указано во введении.

Второй вопрос может быть уточнен путем преобразования тезиса Чёрча–Тьюринга в физический закон:

Изменение любой реальной конечной физической системы может быть как угодно точно сымитировано на вычислительной машине, работающей с универсальными моделями, за конечное число шагов.

Этот закон опирается на закон Дойча (1985). Идея заключается в том, чтобы рассматривать этот закон не как следствие положений квантовой механики, а подобно другим законам (например, закону сохранения энергии), как ее фундамент. Определение «реальная конечная» и «конечное число шагов» имеют значение при формулировке каких-либо положений.

Новый вариант тезиса Чёрча–Тьюринга (который теперь называется «закон Чёрча–Тьюринга») не имеет отношения к машинам Тьюринга. Это очень важно, поскольку между самой природой машины Тьюринга и законами квантовой механики существуют фундаментальные различия. Машина Тьюринга описывается на языке действий с классическими битами, а квантовая механика — на языке эволюций классических состояний. Поэтому существует вероятность того, что машина Тьюринга, а следовательно, и все классические компьютеры, не сможет сымитировать некоторые явления, существующие в Природе. С другой стороны, физически возможно (т.е. нет ограничений со стороны законов Природы) реализовать новый вид вычислений, существенно отличающийся от вычислений, определяемых классической информатикой. Именно эту цель ставят перед собой квантовые вычисления.

4.1. Парадокс Эйнштейна–Подольского–Розена (EPR). Неравенство Белла

В 1935 г. Эйнштейн, Подольский и Розен (EPR) обратили внимание на одну важную особенность нерелятивистской квантовой механики. Сегодня считается, что их выводы, а также анализ Белла, дали импульс

к появлению квантовой теории информации. С парадоксом EPR должен быть знаком любой выпускник-физик, поэтому здесь не будет подробно излагаться его суть. Однако указание его основных положений будет полезно для перехода к понятиям квантовой теории информации.

По своей сути мысленный эксперимент EPR может быть сведен к рассмотрению пар квантовых систем с двумя состояниями (Bohm, 1951; Bohm and Aharonov, 1957). Рассмотрим пару частиц A и B со спином-$\frac{1}{2}$. Будем обозначать состояние «спин вверх» ($m_z = \frac{1}{2}$) как $|\uparrow\rangle$, а состояние «спин вниз» ($m_z = -\frac{1}{2}$) как $|\downarrow\rangle$. Изначально частицы находятся в синглетном состоянии $(|\uparrow\rangle|\downarrow\rangle - |\downarrow\rangle|\uparrow\rangle)\sqrt{2}$, затем они разлетаются и движутся в противоположных направлениях вдоль оси Oy. Алиса и Боб, находясь на значительном расстоянии друг от друга, принимают частицы A и B соответственно. Эйнштейн, Подольский и Розен поставили вопрос о том, способна ли квантовая механика дать полную характеристику частиц либо описание некоторых свойств, например, свойство спиновых моментов количества движения s_A, s_B, которые квантовая механика определить не может, упускается из виду. Подобное утерянное свойство стало называться «скрытой переменной». Авторы парадокса утверждали, что поскольку данный эксперимент позволяет однозначно предсказать результаты измерений любой составляющей спинового момента количества движения s_B без нарушения состояния частицы B, то некоторые характеристики упускаются из виду. Таким образом, считали они, все составляющие момента количества движения s_B имеют определенные значения, а квантовая теория дает лишь неполное описание. Для точного прогноза, без нарушения состояния частицы B, необходимо выбрать ось $O\eta$, относительно которой требуется определить момент количества движения данной частицы, а затем, посредством устройства Штерна–Герлаха (Stern–Gerlach), ориентированного вдоль данной оси, измерить не частицу B, а частицу A. Поскольку суммарный момент количества движения синглетного состояния равен нулю, то можно точно сказать, что соответствующее измерение частицы B дает результат, противоположный результату, полученному при измерении частицы A.

Значимость работы EPR заключатся в том, что она содержит тщательно подобранные доказательства и в ней очень непросто обнаружить ошибку. Существует две возможности для выражения данного ошибоч-

ного вывода: либо можно считать, что измерения Алисы никак не влияют на частицу Боба, либо (что является для меня более предпочтительным) считать, что вектор квантового состояния $|\phi\rangle$ не является внутренним свойством квантовой системы, а определяет объем информации, содержащейся в квантовой переменной. В синглетном состоянии A и B связаны общей информацией, поэтому объем информации, содержащийся в B, изменяется, как только становится известно что либо относительно частицы A. До настоящего момента вышеописанное не отличается от поведения классической информации, и поэтому ничто не выходит за ее рамки.

Более тщательный анализ эксперимента EPR приводит к совершенно неожиданным результатам. Впервые они были найдены Беллом (1964, 1966). Предположим, что Алиса и Боб измеряют составляющие спина относительно различных осей $O\eta_A$ и $O\eta_B$ в плоскости xOz. Результатом каждого измерения является «+» или «−». Квантовая теория согласуется с экспериментом в том, что вероятность появления для двух измерений одинакового результата равна $\sin^2((\phi_A - \phi_B)/2)$, где ϕ_A, ϕ_B — угол между осью Oz и осями $O\eta_A$ и $O\eta_B$ соответственно. Однако, не существует способа определения *локальных* свойств, т. е. независимых друг от друга свойств частиц A и B, которые приводят к такой высокой корреляции, при которой результаты будут определенно противоположны друг другу, если $\phi_A = \phi_B$, и определенно равны, если $\phi_A = \phi_B + 180°$. Кроме того, вероятность совпадения результатов, например, равна $\sin^2(60°) = \frac{3}{4}$, если $\phi_A - \phi_B = 120°$. Фейнман (1982) после проведения тщательного анализа показал, что наивысшая корреляция, обеспечиваемая локальными скрытыми переменными, при $\phi_A - \phi_B = 120°$ равна $\frac{2}{3}$.

Доказательство Bell-EPR позволяет определить физически возможную, но неразрешимую с помощью классического компьютера задачу: когда на вход двух как угодно далеко отстоящих друг от друга точек периодически подаются значения ϕ_A, ϕ_B, то ответы да/нет (время ответа значительно меньше времени прохождения света между данными точками) полностью коррелируют, если $\phi_A = \phi_B + 180°$; противоположно коррелируют, если $\phi_A = \phi_B$, и коррелируют с вероятностью, большей $\sim 70\%$, если $\phi_A - \phi_B = 120°$.

Экспериментальные проверки доказательства Белла были проведены в 1970-х и 1980-х годах. В ходе этих проверок была подтверждена

правильность положений квантовой теории (Clauser and Shimony 1978, Aspect et. al. 1982; более поздние работы: см. Aspect (1991), Kwait et. al 1995, а также ссылки в данных работах). Данные эксперименты стали серьезной проверкой логической структуры квантовой механики. Само доказательство станет более строгим при рассмотрении более сложной системы. В частности, для случая трех спинов, представленных в таком состоянии, как $(|\uparrow\rangle|\uparrow\rangle|\uparrow\rangle + |\downarrow\rangle|\downarrow\rangle|\downarrow\rangle)/\sqrt{2}$ Гринбергер, Хорн и Зейлингер (Greenberger, Horne, Zeilinger, 1989) (GHZ) показали, что одно изменение по горизонтальной оси, проведенное для первых двух частиц, и по вертикальной оси — для третьей частицы, определенно даст результат, противоположный тому, который предсказывает теория скрытой переменной. Более подробное изложение и ссылки можно найти у Гринбергера (Greenberger et. al., 1990) и Мермина (Mermin, 1990).

Корреляции Bell-EPR показывают, что квантовая механика допускает по крайней мере одну задачу, решение которой выходит за рамки возможностей классических компьютеров. Кроме того, они указывают на новый тип общей информации (Schumacher and Nielsen, 1996). Для понимания этих идей необходимо создать завершенную квантовую теорию информации.

Глава 5
Квантовая информация

Как и в случае с классической теорией информации, наилучшим образом показать идеи квантовой теории информации можно путем их взаимосвязи. Квантовая связь рассматривается в специальном издании J. Mog. Opt., том 41 (1994); обзорные статьи и ссылки по криптографии даны Беннеттом (Bennett et. al. 1992), Хагесом (Hughes et. al. 1995), Фениксом и Таунсендом (Phoenix and Townsend, 1995), Брассардом и Крепеау (Brassard and Crepeau, 1996); Экертом (Ekert, 1997). Шпиллер (Spiller, 1996) делает обзор как по связи, так и по вычислениям.

5.1. Кубиты

Элементарной единицей квантовой информации является *кубит* (Schumacher, 1995). Один кубит может рассматриваться как система с двумя состояниями (например, спин-$\frac{1}{2}$) либо как двухуровневый атом (см. рис. 12), однако при определении в кубитах объема квантовой информации совершается более абстрактное действие: говорится, что квантовая система содержит n кубитов, если она содержит 2^n-мерное гильбертово пространство и, таким образом, для нее доступно 2^n *взаимно ортогональных* квантовых состояний (напомним, что n классических битов могут представлять до 2^n различных чисел). Данное определение кубита будет дано более подробно в разделе 5.6.

Будем записывать два ортогональных состояния одного кубита как $\{|0\rangle, |1\rangle\}$. Для более общего случая 2^n ортогональных состояний могут быть записаны как $\{|i\rangle\}$, где i — n-битное двоичное число. Например, в случае с тремя кубитами получим: $\{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\}$.

5.2. Квантовые гейты

Простые унитарные операции над кубитами называются квантовыми «логическими гейтами» (Deutsch 1985, 1989). Например, если ку-

бит переходит из одного состояния в другое $|0\rangle \to |0\rangle$, $|1\rangle \to \exp(i\omega t)|1\rangle$, то говорится, что по прошествии времени t на кубит воздействовали гейтом:

$$P(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}, \tag{22}$$

где $\theta = \omega t$. Данное выражение может быть записано в виде $P(\theta) = |0\rangle\langle 0| + \exp(i\theta)|1\rangle\langle 1|$. Ниже показаны другие элементарные квантовые гейты:

$$I \equiv |0\rangle\langle 0| + |1\rangle\langle 1| = \text{эквивалентность} \tag{23}$$

$$X \equiv |0\rangle\langle 1| + |1\rangle\langle 0| = \text{НЕ (NOT)} \tag{24}$$

$$Z \equiv P(\pi) \tag{25}$$

$$Y \equiv XZ \tag{26}$$

$$H \equiv \frac{1}{\sqrt{2}}\left[(|0\rangle + |1\rangle)\langle 0| + (|0\rangle - |1\rangle)\langle 1|\right]. \tag{27}$$

Все они, являясь единичными операторами, действуют на один кубит и могут быть реализованы посредством какого-либо гамильтониана в уравнении Шредингера[1]. В отличие от классической теории информации, предусматривающей существование только двух гейтов, действующих на один бит: гейт «исключающее ИЛИ-НЕ» и логическая операция НЕ (NOT); в квантовой теории информации существует бесконечное количество однокубитовых квантовых гейтов. Квантовый гейт НЕ аналогичен классическому и преобразует $|0\rangle$ в $|1\rangle$, и наоборот. Данный гейт также называется X гейтом, поскольку является оператором Паули σ_x. Следует отметить, что множество гейтов $\{I, X, Y, Z\}$ является группой по умножению.

Из всего множества возможных унитарных операторов интерес представляет подмножество, которое имеет вид $|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$, где I — однокубитовая операция эквивалентности, а U — какой-либо однокубитовый гейт. Такой гейт носит название «controlled U», поскольку воздействие гейтов I или U на второй кубит контролируется состоянием ($|0\rangle$ или $|1\rangle$) первого кубита. Например, действие гейта controlled-

[1]Здесь для последнего гейта используется заглавная буква H, поскольку воздействие гейта является преобразованием Адамара. Не следует путать его с гамильтонианом $\mathscr{H}$.

NOT (CNOT) записывается в виде

$$\begin{aligned} |00\rangle &\to |00\rangle \\ |01\rangle &\to |01\rangle \\ |10\rangle &\to |11\rangle \\ |11\rangle &\to |10\rangle. \end{aligned} \tag{28}$$

Здесь второй кубит «проходит» через операцию НЕ только в том случае, когда первый кубит находится в состоянии $|1\rangle$. Данный перечень изменения состояний аналогичен таблице истинности классического двоичного логического гейта. Операция (с двумя входами) controlled-CNOT над состоянием $|a\rangle|b\rangle$ может быть записана как $a \to a$, $b \to a \oplus b$, где $\oplus$ обозначает операцию «исключающее ИЛИ» (XOR). По этой причине данный гейт также называется XOR-гейтом.

Другие логические операции требуют большего количества кубитов. Например, операция И (AND) реализуется посредством трехкубитового гейта controlled-controlled-CNOT, в котором над третьим кубитом производится операция НЕ, только если два других находятся в состоянии $|1\rangle$. Данный гейт назван в честь Тоффоли (Toffoli 1980), который показал, что классический вариант является универсальным для классических обратимых вычислений. Действие данного гейта на состояние $|a\rangle|b\rangle|0\rangle$ выражается как $a \to a$, $b \to b$, $0 \to a \cdot b$. Другими словами, гейт выполняет операцию И (AND) над двумя первыми кубитами, если третий кубит находится в состоянии $|0\rangle$. Здесь присутствие трех кубитов необходимо для того, чтобы вся операция в целом была единична и, таким образом, соответствовала квантово-механической эволюции.

Само нахождение последовательности комбинации гейтов для реализации таких элементарных арифметических операций, как двоичное сложение и умножение, является увлекательной задачей. Большое количество основных схем было предложено Баренцо (Barenco et. al. 1995b), а более глубокое рассмотрение общего случая проектирования схем дано Ведралом (Vedral et. al 1996) и Бекманом (Beckman et. al. 1996).

Общее воздействие последовательности квантовых гейтов может быть записано посредством операторов: например, $X_1 H_2 \mathrm{XOR}_{1,3}|\phi\rangle$, где $|\phi\rangle$ — некоторое состояние из трех кубитов, а индексы при операторах показывают номер кубита, на который они воздействуют. Однако в случае последовательности нескольких квантовых гейтов данное обо-

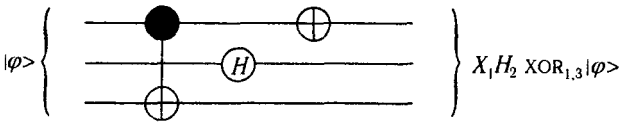

Рис. 8. Пример «квантовой сети». Каждая горизонтальная линия представляет эволюцию одного кубита во времени (движение слева направо). Символ, расположенный на одной линии представляет однокубитовый гейт. Символы, расположенные на двух линиях и соединенные вертикальной чертой представляют двух кубитовые гейтовые операции с данными двумя кубитами. Изображенная на рисунке сеть определяет операцию $X_1H_2\mathrm{XOR}_{1,3}|\phi\rangle$. Символ $\oplus$ представляет функцию X (NOT), H — гейт H; закрашенный круг, соединенный с символом $\oplus$ — операцию controlled NOT

значение становится громоздким и сложным для прочтения, поэтому его заменяют диаграммой, называемой квантовой сетью (см. рис. 8). В последующем будут использоваться именно эти диаграммы.

5.3. Неклонируемость квантового состояния

Теорема неклонируемости. *Неизвестное квантовое состояние не может быть клонировано.*

Эта теорема говорит о том, что нельзя получить точные копии квантового состояния до тех пор, пока оно не определено (т.е. пока не получена классическая информация, характеризующая данное состояние.)

Доказательство.

Для получения копии квантового состояния $|\alpha\rangle$ необходимо подвергнуть пару квантовых систем эволюции, описываемой как: $U(|\alpha\rangle|0\rangle) = |\alpha\rangle|\alpha\rangle$, где U — унитарный оператор эволюции. Если это условие выполняется для любого состояния, то оператор U не должен зависеть от α и, следовательно, $U(|\beta\rangle|0\rangle) = |\beta\rangle|\beta\rangle$ для $|\beta\rangle \neq |\alpha\rangle$. Однако для состояния $|\gamma\rangle = (|\alpha\rangle + |\beta\rangle)/\sqrt{2}$ получим $U(|\gamma\rangle|0\rangle) = (|\alpha\rangle|\alpha\rangle + |\beta\rangle|\beta\rangle)/\sqrt{2} \neq |\gamma\rangle|\gamma\rangle$, а следовательно, операция клонирования не выполняется. Этот вывод применим к любому предложенному методу клонирования (Wooters and Zurek 1982, Dieks 1982). ■

Следует отметить, что данный оператор «клонирования» U применим к некоторым состояниям (состояния $|\alpha\rangle$ и $|\beta\rangle$ в вышеприведенном

примере). Но поскольку данный оператор сохраняет след, два различных клонируемых состояния должны быть ортогональными: $\langle\alpha|\beta\rangle = 0$. До тех пор, пока неизвестно, принадлежит ли клонируемое состояние к одному из вышеуказанных, нельзя с уверенностью сказать, что какой-либо выбранный оператор U обеспечит его точное клонирование. Все это находится в противоположности с классической информацией, когда устройства, подобные ксероксам, легко делают копии любой предоставляемой информации. Операции CNOT или XOR из уравнения (28) являются операциями копирования для состояний $|0\rangle$ и $|1\rangle$, но не для таких состояний, как $|+\rangle \equiv (|0\rangle + |1\rangle)/\sqrt{2}$ и $|-\rangle \equiv (|0\rangle - |1\rangle)/\sqrt{2}$.

Теорема неклонируемости и парадокс EPR ведут к довольно тонким выводам, в которых теория нерелятивистской квантовой механики играет важную роль. Действительно, если бы клонирование было возможно, то корреляции EPR обеспечили бы связь, чья скорость превышала бы световую. Это, в свою очередь, ведет к противоречию (действие опережает причину), поскольку в расчет принимаются законы специальной теории относительности. Для того чтобы понять это, заметим, что Боб, создав большое количество клонов и измерив их по различным базисам, может однозначно определить, находится ли член пары EPR в состоянии с базисом $\{|0\rangle, |1\rangle\}$ или базисом $\{|+\rangle, |-\rangle\}$. Алиса могла бы обеспечить практически мгновенную связь посредством перевода пары EPR в тот или иной базис в зависимости от ее выбора оси, по которой осуществляется измерение.

5.4. Плотное кодирование

Проанализируем следующее утверждение:

Квантовое зацепление является информационным ресурсом.

Кубиты могут использоваться для хранения и переноса классической информации. Например, для передачи строки классических битов 00101 Алисе потребуется пять кубитов, находящихся в состоянии $|00101\rangle$. Боб, приняв сообщение, может извлечь из него информацию посредством измерения каждого кубита по базису $\{|0\rangle, |1\rangle\}$ (т.е. в результате получаем собственные состояния измеряемой величины). Результаты измерения однозначно определяют данную строку классических битов. При передаче каждого кубита передается информация не более чем об одном классическом бите.

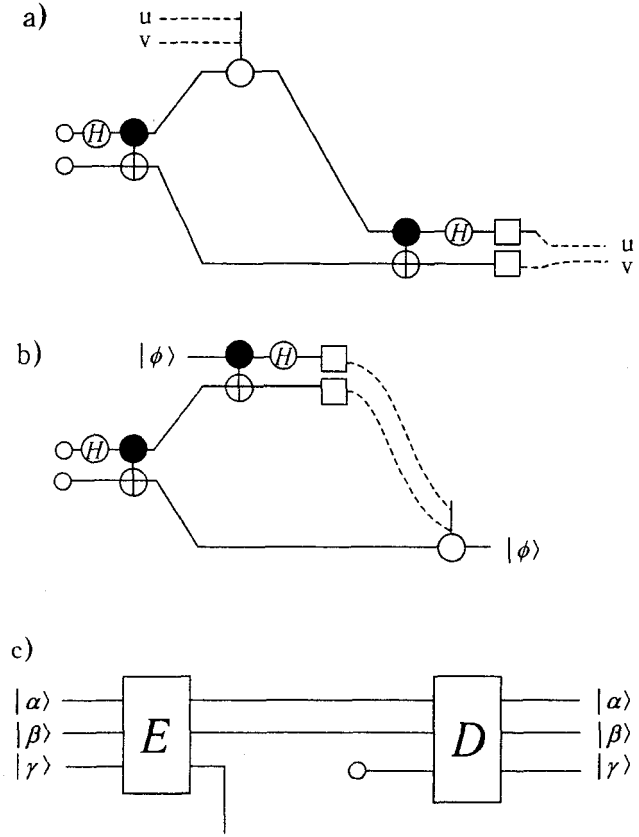

Рис. 9. Основные понятия квантовой связи для a) плотного кодирования, b) телепортации и c) сжатия информации. Расстояние в пространстве между Алисой и Бобом отмечается в вертикальном направлении, течение времени — слева направо. Блоки представляют измерения, пунктирные линии — классическую информацию

Теперь предположим, что Алиса и Боб имеют зацепленную пару кубитов, находящихся в состоянии $|00\rangle+|11\rangle$ (с этого момента для простоты записи будем опускать коэффициент нормирования $\sqrt{2}$). До этого Алисе и Бобу никогда не требовалось устанавливать связь друг с другом: предположим, что существует главное механическое устройство,

которое генерирует зацепленные пары кубитов и направляет каждый из кубитов для хранения Алисе и Бобу (см. рис. 9а). В этом случае Алиса может сообщить Бобу информацию о двух классических битах посредством передачи только одного кубита (т.е. передачи своей части зацепленной пары). Согласно Виснеру (Bennett and Wiesner 1992) данный метод называется «плотным кодированием», поскольку для передачи двух классических битов Алисе нужен лишь один квантовый бит, т.е. несмотря на то, что в операции передачи информации задействовано два кубита, она располагает лишь одним из них. Данный метод опирается на следующий факт: для четырех взаимно ортогональных состояний $|00\rangle + |11\rangle$, $|00\rangle - |11\rangle$, $|01\rangle + |10\rangle$, $|01\rangle - |10\rangle$ переход от одного состояния к другому может быть обеспечен посредством операций с одним кубитом. Данный набор состояний называется базисом Белла, поскольку они проявляют наиболее сильную корреляцию Bell-EPR из всех возможных (Braunstein et. al. 1992). Начиная с состояния $|00\rangle + |11\rangle$, Алиса может получить любое из состояний базиса Белла посредством воздействия на имеющиеся кубиты одним из операторов $\{I, X, Y, Z\}$. Поскольку существует только четыре возможных оператора, то ее выбор воздействия будет определять два бита классической информации. После передачи кубита Боб должен определить в каком из состояний базиса Белла находится данный кубит. Это можно сделать посредством воздействия на пару кубитов гейтом XOR и измерения результирующего бита (target bit). Таким образом, Боб отличит состояния $|00\rangle \pm |11\rangle$ от состояний $|01\rangle \pm |10\rangle$. Для определения знака суперпозиции он должен использовать для оставшегося кубита преобразование Адамара H, а затем произвести измерение результата. Таким образом, Боб однозначно получает информацию о двух классических битах.

Плотное кодирование сложно осуществимо и не имеет практического значения, кроме стандартного метода связи. Однако данный метод обеспечивает защиту связи: получить информацию, содержащуюся в двух классических битах, можно только в том случае, если кто-либо обладает кубитом, парным к кубиту, отправляемому Алисой. В общем случае плотное кодирование соответствует утверждению, помещенному в начале данного раздела. Оно показывает взаимосвязь между классической информацией, кубитами и количеством информации в квантовом зацеплении (Barenco and Ekert 1995). Лабораторная демонстрация основных свойств описана Mattle et. al. (1996).

5.5. Квантовая телепортация

Возможно передавать кубиты, не отправляя их!

Предположим, что Алиса хочет передать Бобу один кубит в состоянии $|\phi\rangle$. Если ей уже известно состояние кубита, например $|\phi\rangle = |0\rangle$, то она может передать его Бобу с помощью классической информации: «Дорогой Боб, кубит находится в состоянии $|0\rangle$. С уважением, Алиса». Однако, если состояние $|\phi\rangle$ неизвестно, то она не может точно его определить: любое измерение с ее стороны может вызывать изменение состояния; кроме того, Алиса не может клонировать его, для того, чтобы провести измерения на копиях данного состояния. Очевидно, что единственный способ передать бобу состояние $|\phi\rangle$ — это оправить ему физический кубит (т.е. электрон, или атом, или что-либо еще) либо перевести данное состояние в другую квантовую систему и отправить ее. В любом случае будет осуществлена передача квантовой системы.

Выход из этих ограничений заключается в использовании метода квантовой телепортации (Bennett et. al. 1993, Bennett 1995). Как и в случае плотного кодирования, будем использовать квантовое зацепление в качестве источника информации. Предположим, что у Алисы и Боба имеется зацепленная пара кубитов в состоянии $|00\rangle + |11\rangle$. Алиса должна передать Бобу один кубит, находящийся в неизвестном состоянии $|\phi\rangle$. В самом общем случае можно написать: $|\phi\rangle = a|0\rangle + b|1\rangle$, где a и b — неизвестные коэффициенты. Следовательно, начальное состояние трех кубитов выражается как:

$$a|000\rangle + b|100\rangle + a|011\rangle + b|111\rangle. \tag{29}$$

После этого Алиса измеряет по базису Белла первые два кубита, т. е. она измеряет неизвестный кубит и один кубит из зацепленной пары. Квантовая сеть для этой операции показана на рис. 9b. После применения Алисой гейтов XOR и гейта Адамара, но до измерения кубитов, получаем следующее состояние:

$$|00\rangle(a|0\rangle + b|1\rangle) + |01\rangle(a|1\rangle + b|0\rangle) + \\ + |10\rangle(a|0\rangle - b|1\rangle) + |11\rangle(a|1\rangle - b|0\rangle). \tag{30}$$

В результате измерения, проводимого Алисой, осуществляется замена данного состояния на одно из четырех возможных и происходит выделение двух классических битов. Данные два бита передаются Бобу,

и он с их помощью определяет, какой из операторов $\{I, X, Y, Z\}$ ему необходимо применить к своему кубиту для того, чтобы поместить его в состояние $a|0\rangle + b|1\rangle = |\phi\rangle$. Таким образом, Боб детектирует кубит (т. е. квантовую информацию, а не реальную квантовую систему), который должна была передать Алиса.

Следует отметить, что квантовая информация передается Бобу только в том случае, если она исчезает у Алисы (свойство неклонируемости). Кроме того, квантовая информация является полной, поскольку состояние $|\phi\rangle$ — это полное описание кубита Алисы. А термин «телепортация» обращает внимание на два вышеуказанных факта. Идея телепортации становится существенной при рассмотрении в разделе 9 связи с помехами.

5.6. Сжатие квантовой информации

После того как было введено понятие кубита, необходимо показать, что он является удобной мерой количества квантовой информации. Данное доказательство было выполнено Джозса и Шумахером (Jozsa and Schumacher 1994), которые опирались на работы Холево (Kholevo 1973) и Левитина (Levitin 1987). Перед началом доказательства необходимо выбрать величину, показывающую, какой объем информации можно получить при определении квантового состояния некоторой системы Q. Приемлемой является величина энтропии фон Неймана (Von Neumann)

$$S(p) = -\operatorname{Tr} \rho \log \rho, \tag{31}$$

где Tr — частичный след оператора, а ρ — оператор сложности, определяющий совокупность состояний квантовой системы. Это выражение необходимо сравнить с уравнением (1), выражающим классическую энтропию Шеннона. Предположим, что классическая случайная переменная X подчиняется закону распределения вероятностей $p(x)$. Если квантовая система находится в состоянии $|x\rangle$, которое определяется значением величины X, то матрица плотности выражается как $\sum\limits_x p(x)|x\rangle\langle x|$, причем состояния $|x\rangle$ не обязательно должны быть ортогональными. Можно показать, что энтропия $S(p)$ ограничивает сверху количество классической общей информации $I(X : Y)$ для величины X и результата измерения системы Y.

Для перехода к кубитам рассмотрим ресурсы, необходимые для хранения и передачи состояния квантовой системы q, задаваемой матрицей плотности ρ. Идея состоит в накоплении подобных систем (их количество $n \gg 1$) и переноса («кодирования») совместного состояния на какую-либо систему более низкого порядка. Данная система передается по каналу связи и при ее получении, совместное состояние «декодируется» в n систем q', подобных системе q (см. рис. 9с). Каждая система q' задается матрицей плотности ρ', а сам процесс передачи считается успешно завершенным, если матрица ρ' достаточно точно повторяет матрицу ρ. Мерой подобия матриц плотности является *точность* передачи:

$$f(\rho, \rho') = (\mathrm{Tr}\sqrt{\rho^{1/2}\rho'\rho^{1/2}})^2. \qquad (32)$$

Данное выражение может рассматриваться как вероятность прохождения матрицей ρ' проверки на ее совпадение с матрицей ρ. В случае, когда обе матрицы ρ и ρ' определяют чистые состояния: $|\phi\rangle\langle\phi|$ и $|\phi'\rangle\langle\phi'|$, точность передачи является ни чем иным, как хорошо известным перекрытием: $f = |\langle\phi|\phi'\rangle|^2$.

В данном случае задача заключается в определении системы наименьшего порядка с точностью передачи $f = 1 - \varepsilon$ при $\varepsilon \ll 1$. Доказательство аналогично идее «типичных последовательностей», приведенной в разделе 2.2. Ограничиваясь для простоты рассмотрением систем с двумя состояниями, найдем, что полное состояние n систем описывается вектором в 2^n-мерном гильбертовом пространстве. Однако, если величина энтропии фон Ньюмана $S(\rho) < 1$, то существует высокая вероятность (т. е. вероятность стремится к единице при достаточно большом n) того, что при любой заданной реализации вектор состояния фактически перейдет в *типичное подпространство* гильбертова пространства. Шумахер и Джозса показали, что размерность данного типичного подпространства равна $2^{nS(\rho)}$. Следовательно, для точного представления квантовой информации требуется только $nS(\rho)$ кубитов, а сам кубит (т. е. логарифм размерности гильбертова пространства) является удобной мерой квантовой информации. Более того, операция кодирования и декодирования «беспристрастна»: она не зависит от количества информации, известной относительно передаваемого состояния.

Результаты, полученные Шумахером и Джозса, полезны, поскольку относятся к общему случаю: не было сделано никаких допущений

относительно природы рассматриваемых квантовых состояний. В частности, они могут быть и не ортогональны. В случае же, когда передаваемые состояния взаимно ортогональны, то задача сводится к рассмотрению переноса классической информации.

«Кодирование» и «декодирование», необходимые для достижения подобных сжатия и декомпрессии квантовой информации, требуют серьезного технологического обеспечения. На сегодняшний день невозможно осуществить данные операции для всех используемых фотонов. Однако такое сжатие является максимально возможным с точки зрения законов физики. Точное описание требуемых квантовых сетей определено Клеве (Cleve) и ДиВинченцо (DiVincenzo, 1996).

Как и в случае с основным понятием информации, другие классические идеи, такие, как кодирование Хаффмана, нашли своих квантовых двойников. Кроме того, Шумахер и Нильсон (Neilson, 1996) ввели величину, которую они назвали «когерентной информацией» и которая является мерой общей информации для квантовых систем. Эта величина затрагивает ту часть общей информации между зацепленными системами, которая не имеет классического описания и, кроме того, помогает понять корреляции Bell-EPR.

5.7. Квантовая криптография

Ни один обзор по квантовой информации не является полным, если в нем не упоминается квантовая криптография. Данный раздел берет свое начало от неопубликованной работы Виснера (Wiesner), написанной примерно в 1970 году (Wiesner 1983). В этой работе отображены различные идеи по использованию свойств квантовых систем для решения таких важных задач криптографии, как защита (т. е. секретность) информации во время связи. Из данного раздела можно выделить следующие подразделы: *квантовый протокол передачи ключа* (quntum key distribution) и объединение идей, в общих чертах относящихся к задаче *фиксации битов* (bit commitment). В общих чертах описание квантового протокола передачи ключа будет дано ниже. Фиксацию битов можно отнести к ситуации, когда Алиса должна принять какое-либо решение, например, проголосовать, но так, чтобы Боб был уверен, что она приняла его за определенное время. При этом Боб может узнать о решении Алисы несколько позднее, в то время, которое она сама определит. Классический, но несколько громоздкий метод достижения фиксации

битов заключается в том, что Алиса должна записать на бумаге свое решение, поместить его в сейф, который она после передаст Бобу. Если позднее она захочет, чтобы Боб узнал ее решение, она сообщит ему код сейфа. Типичный квантовый протокол как тщательно разработанная разновидность вышеописанного метода базируется на следующей идее: Алиса передает Бобу кубит, а позднее сообщает ему о том, в каком базисе данный кубит был представлен. Первые статьи о квантовой криптографии были представлены во введении; дополнительные ссылки можно найти в обзорах, упомянутых в начале данного раздела. Криптография обладает одной необычной чертой, заключающейся в том, что невозможно экспериментально доказать защищенность процедуры: никогда неизвестно, удалось ли шпиону или мошеннику взломать систему. С другой стороны, конфиденциальность пользователей должна опираться на математические доказательства защиты связи, и именно в этой области был произведен значительный объем работ. Согласованные усилия позволили доказать защищенность точно осуществленного квантового протокола передачи ключа. Однако недавно была доказана незащищенность связи посредством квантовых методов и опирающейся на идею фиксации битов (Mayers 1997, Lo and Chau 1997); хотя в течение длительного времени данная связь таковой не считалась. Это доказательство следует из того, что участники связи могут использовать в корыстных целях квантовые зацепления.

Квантовый протокол передачи ключа является методом, в котором для определения случайного секретного ключа для криптографии используются квантовые состояния. Как и прежде, Алисе и Бобу, находящимся на значительном расстоянии, необходимо обеспечить связь друг с другом. Алиса передает Бобу $2n$ кубитов, каждый из которых находится в каком-нибудь случайно выбранном состоянии: $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$.[2] Боб измеряет полученные биты также по случайно выбранному базису: $\{|0\rangle, |1\rangle\}$ и $\{|+\rangle, |-\rangle\}$. После этого Алиса и Боб публично (т. е. чтобы все знали об этом) сообщают друг другу о базисах, который каждый из них использовал для представления и измерения кубитов. Они подсчитывают случаи, когда ими случайно был использован один и тот же базис. Данные случаи составляют половину всех проверок и сохраняют результаты, соответствующие только данным случаям. Сейчас, при отсутствии ошибок и интерференции, Алиса и Боб имеют одинако-

[2] Возможны и другие методы. Данный метод был выбран только для того, чтобы проиллюстрировать основные принципы.

вые строки, состоящие из n классических битов (предварительно они должны условиться считать $|0\rangle$ или $|+\rangle$ за 0, $|1\rangle$ или $|-\rangle$ за 1). Данная строка классических битов часто называется *несовершенной квантовой передачей* (raw quantum transmission RQT).

До сих пор использование кубитов не принесло никаких результатов. Однако важной особенностью является то, что никто не сможет узнать о результатах измерения Боба путем наблюдения за кубитами во время их пересылки. Наиболее непродуманным способом, используемым Евой (она следит за передаваемыми кубитами) для определения ключа, является перехват, измерение кубитов и последующая передача их Бобу. В течение примерно половины времени связи Ева точно определяет базис, используемый Алисой и поэтому не нарушает состояния кубита. Однако базисы, используемые Евой не совпадают с базисами, которые применяет Боб. Таким образом, Ева узнает состояние только половины тех n кубитов, которые впоследствии Алиса и Боб сочтут достоверными. Кроме того, она нарушает состояние оставшейся половины, отправляя, например, Бобу состояние $|+\rangle$ вместо состояния $|0\rangle$, отправленного Алисой. Половина кубитов с нарушенными состояниями будут в результате измерения Боба спроецированы обратно в первоначальное состояние, заданное Алисой. В результате Ева нарушает состояние $\frac{n}{4}$ битов строки RQT.

Теперь Алиса и Боб смогут узнать о присутствии Евы посредством случайного выбора $\frac{n}{2}$ битов строки RQT и публичного оглашения их значений. Если все объявленные значения совпадают, Алиса и Боб могут быть уверены, что их никто не подслушивал, поскольку вероятность того, что Ева их подслушивала, а они выбрали $\frac{n}{2}$ битов с ненарушенным состоянием, равна $(3/4)^{n/2} \simeq 10^{-125}$ при $n = 1000$. Эти $\frac{n}{2}$ непрочитанных битов и образуют секретный ключ.

На практике протокол является более сложным, поскольку Ева может использовать различные стратегии подслушивания (например, не перехватывать все кубиты); кроме того, даже при отсутствии прослушивания, помехи неизбежно исказят некоторые из кубитов. Вместо отказа от ключа в случае, когда многие из оглашенных битов не совпадают, Алисе и Бобу нужно пользоваться им до тех пор, пока уровень ошибок не превысит 25%. Последующая обработка ключа состоит из двух шагов. Первый шаг заключается в обнаружении и удалении ошибок посредством публичной проверки на совпадение значений битов из

случайно выбранных последовательностей; с одновременным отказом от битов с целью не допустить получения Евой дополнительной информации. На втором шаге из данного ключа выделяется другой, меньший по длине, составленный из совпадающих значений первоначального ключа. При этом знания Евы о ключе уменьшаются. Таким образом, можно получить новый ключ, составленный примерно из $\frac{n}{4}$ битов, при этом с большой вероятностью знания Евы о данном шифре составляют менее 10^{-6} бита (Bennett et. al. 1992).

Вышеописанный протокол не является единственно возможным. Другой подход (Ekert 1991) связан с использованием пар EPR, которые Алиса и Боб измеряют по одной из трех осей. С целью исключения подслушивания им необходимо, в своих результатах, проверить наличие корреляций Bell-EPR.

Существенное преимущество квантового протокола передачи ключа заключается в том, что он осуществим на данном уровне технологического развития. В самом первом эксперименте (Bennett и Barssard 1989) была показана суть метода, а уже после он был значительно усовершенствован. Два года назад Хагес (Hughes et. al. 1995), Феникс и Таунсенд (Phoenix and Townsend, 1995) подвели итог состоянию дел в данной области, а недавно Збинден (Zbinden et. al. 1997) сообщил об успешной передаче ключа на расстояние в 23 км по стандартному телекоммуникационному волокну, проходящему под озером Женева. Кубиты хранились в поляризованных состояниях лазерных импульсов, т. е. в когерентных световых состояниях, содержащих в среднем 0,1 фотона на импульс. Такой низкий световой уровень был необходим для того, чтобы максимально снизить вероятность появления импульса, содержащего более одного фотона, поскольку подобные импульсы могут воспроизводить кубиты и, таким образом, позволяют подслушивающему оставаться незамеченным. В данной системе был достигнут уровень ошибок битов в 1,35%, что является достаточно низким показателем и обеспечивает защиту протокола. Скорость передачи данных довольно низкая: она измеряется в МГц против обычных для классической связи скоростей, измеряемых в ГГц. Но, несмотря на это, система очень надежна.

Глава 6
Универсальный квантовый компьютер

После ознакомления со всеми выше указанными понятиями можно перейти к рассмотрению квантовой теории информации — квантовому компьютеру (QC). Ознакомительные обзоры, посвященные квантовому компьютеру и задаче разложения числа на множители, были представлены Екертом и Джозса (Ekert, Jozsa 1996) и Баренцо (Barenco 1996). Шпиллер (Spiller 1996) в своем обзоре в основном рассматривал практическое применение квантовых компьютеров. Обзорные материалы можно также найти у ДиВинченцо (1995) и Шора (Shor 1996).

В первую очередь квантовый компьютер является устройством, которое существует лишь в теории, в мысленном эксперименте, чья задача сводится к формальному анализу обработки квантовой информации. В частности, с помощью данных теоретических построений можно вывести закон Чёрча–Тьюринга, рассмотренный в разделе 4.

Опираясь на работы Дойча (1985, 1989), ниже даются требования, предъявляемые квантовому компьютеру:

Квантовый компьютер представляет множество, состоящее из n кубитов, для которого практически определены следующие операции:

1. Каждый кубит может быть представлен в каком-либо известном состоянии $|0\rangle$.

2. Каждый кубит может быть измерен по базису $\{|0\rangle, |1\rangle\}$.

3. Универсальный квантовый гейт (или множество гейтов) может воздействовать на любое ограниченное подмножество кубитов.

4. Состояние кубитов не изменяется кроме как посредством вышеуказанных преобразований.

Данное описание не затрагивает определенных технологических сторон, которые будут обсуждаться в дальнейшем, но содержит основные идеи квантового компьютера.

Теоретическая модель вычислений является сетевой. В ней осуществляется последовательное воздействие логическими гейтами на множество битов (здесь: квантовых битов). Логические гейты классического электронного компьютера расположены на монтажной плате

отдельно друг от друга, в квантовом компьютере логические гейты рассматриваются как взаимодействия кубитов, происходящие в определенное время. При этом кубиты, как показано на диаграммах квантовых сетей (рис. 8, 12), занимают неизменное положение. Возможна проработка и других моделей квантовых вычислений — например, модели клеточного автомата (Margolus 1990).

6.1. Универсальный гейт

Универсальный квантовый гейт является квантовым эквивалентом универсального классического гейта, т. е. гейта, который, воздействуя на различные комбинации битов, может имитировать действие любого другого гейта. Однако, что из себя представляет множество всех возможных квантовых гейтов? Для ответа на этот вопрос нужно обратиться к принципам квантовой механики (уравнение Шредингера): поскольку квантовая эволюция единична, будет достаточно создать в компьютере *все единичные преобразования* n кубитов. На первый взгляд это может показаться трудной задачей, поскольку имеется непрерывное, а следовательно, бесконечное множество. Однако, как показал Дойч в 1985 г., довольно простые квантовые гейты могут быть универсальными.

Работу универсального гейта можно показать на следующем простом примере. Рассмотрим пару гейтов: $V(\theta, \phi)$ и «controlled-NOT» (или XOR), где $V(\theta, \phi)$ — гейт произвольного вращения одного кубита, т. е.

$$V(\theta, \phi) = \begin{Bmatrix} \cos(\theta/2) & -ie^{-i\phi}\sin(\theta/2) \\ -ie^{-i\phi}\sin(\theta/2) & \cos(\theta/2) \end{Bmatrix}. \qquad (33)$$

Можно показать, что любая единичная матрица размерности $n \times n$ может быть образована путем комбинирования двухкубитовых гейтов XOR и гейтов вращений одного кубита. Таким образом, данная пара операций может рассматриваться в квантовых вычислениях как универсальная.

Можно возразить, что гейт $V(\theta, \phi)$ должен рассматриваться как бесконечное множество гейтов, поскольку его параметры являются непрерывными. Однако, посредством выбора двух определенных иррациональных значений углов θ и ϕ и многократного применения гейта с данными значениями, можно описать практически все вращения одного

кубита. Однако нет необходимости использовать подобные трудоемкие методы в реальной системе — путем комбинирования операций вращения и XOR, можно описать операцию контролируемого вращения, являющуюся одиночным универсальным гейтом. Описание подобных универсальных гейтов можно найти у Дойча (Deutsch et. al. 1995), Ллойда (Lloyd 1995), Ди Винченцо (DiVincenzo 1995a) и Баренцо (Barenco 1995).

Следует отметить, что двухкубитовые гейты достаточны для выполнения квантовых вычислений. Именно поэтому квантовый гейт является мощным и важным понятием.

6.2. Закон Чёрча–Тьюринга

Ознакомившись с квантовым компьютером, необходимо доказать его универсальность, т. е. показать, что он функционирует в соответствии с законом Чёрча–Тьюринга. Доказательство состоит из двух шагов и само по себе очень простое. Во-первых, состояние любой квантовой системы есть вектор в гильбертовом пространстве. Таким образом, оно может быть представлено как угодно точно с помощью конечного числа кубитов. Во-вторых, эволюция любой квантовой системы есть единичное преобразование и, таким образом, она может быть сымитирована на квантовом компьютере, который способен создавать новое единичное преобразование с произвольной точностью.

Принципиальный вопрос был затронут Мейерсом (1997), когда он определил, что вычислительные задачи, для которых не определено количество шагов до завершения, представляют определенные трудности. В противоположность классическому компьютеру нельзя определить останов квантового компьютера. Однако в дальнейшем будут рассматриваться либо задачи, у которых можно прогнозировать число шагов до завершения, либо задачи, об останове которых квантовый компьютер сообщает с помощью специально предназначенного для этого кубита, не задействованного в вычислениях (Deutsch 1985).

Несмотря на вышеуказанные условия, остается очень широкий круг задач для рассмотрения. Нильсен и Чуанг (Nielsen and Chuang 1997) рассмотрели применение массива *фиксированных* квантовых гейтов и показали, что если с помощью массива можно оперировать кубитами, являющимися одновременно информацией и программой, то невозможно посредством этого же массива осуществлять единичное преобразование информации. Однако ниже будут рассмотрены устройст-

ва, в которых классический компьютер управляет квантовыми гейтами, действующими на квантовый регистр. Таким образом, с помощью классической программы можно «определять» любой массив (любую последовательность) гейтов и направлять его в квантовый компьютер.

Без сомнения, квантовый компьютер является познавательным теоретическим инструментом. Но рядом с ним до сих пор стоит большой знак вопроса, требующий ознакомиться с его неидеальностью. Описания квантового компьютера, указанные выше, относятся к случаю, когда при выполнении измерений или применении гейтов может быть достигнута любая точность. Данные случаи, как и четвертое требование (отсутствие эволюции извне), являются физически некорректными. Описание квантового компьютера будет реалистичным, если к каждому их четырех требований добавить положение относительно допустимой степени точности. Данный вопрос является предметом сегодняшних исследований, которые будут рассмотрены в разделе 9. Пока же необходимо более подробно изучить возможности тщательно спроектированного квантового компьютера.

Глава 7
Квантовые алгоритмы

Общеизвестно, что классические компьютеры способны рассчитать поведение квантовых систем, однако до сих пор не было показано, что квантовый компьютер может работать с задачами, неразрешимыми для классического компьютера. Действительно, поскольку физические теории содержат уравнения, которыми можно оперировать, то кажется очень маловероятным тот факт, что квантовая механика или какая-либо физическая теория, которая может появиться в будущем, смогут допустить существование вычислительных задач, неразрешимых в принципе с помощью довольно большой классической машины Тьюринга. Однако, как было показано в разделе 3.2, определения «довольно большая» и «достаточно быстрая» играют ключевую роль в информатике. Задачи, «сложные» с точки зрения вычислений, на практике могут оказаться просто неразрешимыми. Говоря более строго, до тех пор, пока квантовые вычисления не расширят множество решаемых задач (по сравнению с классическими вычислениями) можно говорить о возможности появления нового класса сложности. Другими словами, задачи, которые не могут быть адресованы классическому компьютеру по причине его медленной работы, могут быть решены с помощью квантового компьютера.

7.1. Имитация физических систем

Первым и наиболее очевидным применением квантовых компьютеров является имитация каких-либо других квантовых систем. Для имитации вектора состояния в 2^n-мерном гильбертовом пространстве классическому компьютеру необходимо оперировать векторами, содержащими порядка 2^n комплексных чисел. Для той же цели квантовому компьютеру требуется лишь n кубитов, что делает его более эффективным с точки зрения необходимого объема памяти. Однако в общем случае и квантовый, и классический компьютеры неэффективны для

имитации эволюции системы. Классический компьютер должен оперировать матрицами, содержащими 2^{2n} элементов, при этом число операций (умножение, сложение) экспоненциально зависит от n. В свою очередь число элементарных квантовых логических гейтов экспоненциально зависит от числа единичных операций квантового компьютера, осуществляемых в 2^n-мерном гильбертовом пространстве. Таким образом, квантовый компьютер не может гарантировать эффективную имитацию любой физической системы. Однако можно показать, что квантовый компьютер эффективен при имитации большого класса квантовых систем, для многих из которых, например для систем многих тел с локальными взаимодействиями, не существует эффективного классического алгоритма решения (Lloyd 1996, Zalka 1996, Wiesner 1996, Meyer 1996, Lidar и Biam 1996, Abrams and Lloyd 1997, Boghosian and Taylor 1997).

7.2. Алгоритм поиска периода функции. Алгоритм Шора по разложению на множители

До настоящего момента в обзоре рассматривалась лишь имитация процессов Природы, что является довольно ограниченным типом вычисления. Хотелось бы, чтобы квантовый компьютер использовался и для решения более общих задач; хотя и было доказано, что поиск тех задач, в которых квантовый компьютер был бы эффективнее классического, затруднителен. Однако факт, что подобные задачи, в принципе, существуют, является значительным открытием в физике. Он также в большой степени способствовал поискам в данной области.

На сегодняшний день алгоритм поиска периода функции является одним из самых важных. Предположим, что функция $f(x)$ — периодическая с периодом r, т.е. $f(x) = f(x + r)$. Предположим далее, что функция $f(x)$ может быть легко найдена при данном x, кроме того, изначально известно, что $N/2 < r < N$ для какого-либо N. Предполагая, что не существует аналитического способа определения периода функции $f(x)$, единственным выходом остается определение с помощью классического компьютера значений $f(x)$ для порядка $N/2$ значений x, и нахождение того значения x, после которого значения функции начинают повторяться (для регулярных функций необходимо в среднем лишь $O(\sqrt{N})$ значений). Данный метод является неэффективным, по-

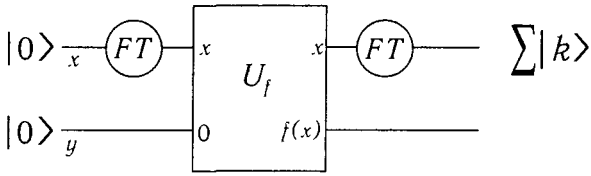

Рис. 10. Квантовая сеть для алгоритма Шора по нахождению периода функции. Здесь каждая горизонтальная линия обозначает квантовый регистр, а не кубит. Окружности слева представляют создание входного состояния $|0\rangle$. Символ FT в кружочке представляет преобразование Фурье (см. текст), а блок, связывающий два регистра, представляет сеть, соответствующую оператору U_f. Действие алгоритма завершается после измерения регистра x

скольку число операций экспоненциально зависит от величины $\log N$ (информации, необходимой для определения N).

Вышеуказанная задача может быть решена на квантовом компьютере посредством строгого метода (см. рис. 10), предложенного Шором (1994) и опирающегося на метод Симона (1994). Для решения задачи квантовому компьютеру необходимо $2n$ кубитов, а также $O(n)$ кубитов — для создания рабочего пространства, где $n = [2\log N]$ (выражение $[n]$ обозначает ближайшее бóльшее целое к x число). Все кубиты делятся на два «регистра», каждый из которых содержит по n кубитов. Ниже будем обращаться к ним, как к «регистру x» и «регистру y». Каждый из регистров изначально задан в состоянии $|0\rangle$ (т. е. все n кубитов находятся в состоянии $|0\rangle$). Далее, к каждому из кубитов регистра x применим операцию H, определяя итоговое состояние

$$\frac{1}{\sqrt{\omega}} \sum_{x=0}^{\omega-1} |x\rangle|0\rangle, \tag{34}$$

где $\omega = 2^n$. По причинам, которые вскоре станут очевидными, данное действие рассматривается как преобразование Фурье (см. рис. 10). Выражение $|x\rangle$ обозначает, например, состояние $|0011010\rangle$, где 0011010 — двоичная запись целого числа x. В связи с этим базис $\{|0\rangle, |1\rangle\}$ может рассматриваться как «вычислительный базис». При описании компьютера удобно (хотя, разумеется, не обязательно) пользоваться данным базисом. Затем, для выполнения преобразования $U_f|x\rangle|0\rangle = |x\rangle f|x\rangle$, к регистрам x и y применяется сеть логических гейтов. Следует от-

метить, что данное преобразование может быть единичным, поскольку входное состояние $|x\rangle|0\rangle$ полностью соответствует входному состоянию $|x\rangle|f(x)\rangle$, и, следовательно, процессы являются обратимыми. Теперь, применяя преобразование U_f к состоянию, описываемому уравнением (34), получим

$$\frac{1}{\sqrt{\omega}} \sum_{x=0}^{\omega-1} |x\rangle|f(x)\rangle. \tag{35}$$

Данное состояние продемонстрировано на рис. 11а. Здесь необходимо отметить следующую уникальную особенность: за один шаг были найдены значения функции $f(x)$ для $\omega = 2^n$ значений x. Эта особенность называется *квантовым параллелизмом* и, вследствие экспоненциальной зависимости от n, представляет мощнейший параллелизм. (Вообразите существование 2^{100}, т. е. в миллион раз больше числа Авогадро, классических процессоров).

Хотя 2^n значений функции $f(x)$ в каком-то смысле «присутствуют» в квантовом состоянии, определяемом уравнением (35), прямой доступ к ним, к сожалению, невозможен. Это связано с тем, что в соответствии со следующим шагом алгоритма, вследствие измерения (по вычислительному базису) регистра y можно получить лишь одно значение $f(x)$.[1] Предположим, что при этом получаем значение функции $f(x) = u$. Состояние регистра y перебрасывается в состояние $|u\rangle$, а общее состояние будет определяться как

$$\frac{1}{\sqrt{M}} \sum_{i=0}^{M-1} |d_u + jr\rangle|u\rangle, \tag{36}$$

где $d_u + jr$ — все значения x, для которых $f(x)=u$, $j = 0, 1, 2, \ldots, M-1$. Другими словами, периодичность функции $f(x)$ означает, что регистр x является суперпозицией $M \simeq \omega/r$ состояний при значениях x, взятых с периодом r. Следует отметить, что смещение d_u множества значений x зависит от величины u, полученной при изменении регистра y.

Теперь необходимо определить периодичность состояния в регистре x. Для этого необходимо последовательно осуществить преобразова-

[1] Нет необходимости в обязательном измерении регистра y. Однако данное действие упрощает описание.

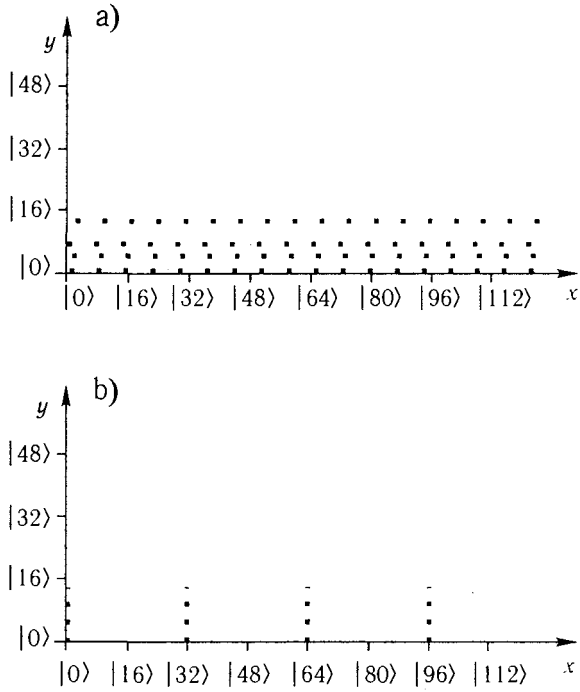

Рис. 11. Эволюция квантового состояния, соответствующая алгоритму Шора. Схематично квантовое состояние показано посредством определения ненулевых требований к суперпозиции. Таким образом, общее состояние $\sum c_{x,y}|x\rangle|y\rangle$ изображается закрашенным квадратом в тех точках с координатами (x, y), для которых $c_{x,y} \neq 0$. Рис. a) соответствует уравнению (35), b) — уравнению (38)

ние Фурье и измерение состояния. Используемое дискретное преобразование Фурье описывается следующей единичной процедурой

$$U_{\mathcal{FT}}|x\rangle = \frac{1}{\sqrt{\omega}} \sum_{k=0}^{\omega-1} e^{i2\pi kx/\omega}|k\rangle. \qquad (37)$$

Отметим, что уравнение (34) является примером данной процедуры, примененной к начальному состоянию $|0\rangle$. Основой для квантовой сети, необходимой для реализации преобразования $U_{\mathcal{FT}}$, служит алгоритм

быстрого преобразования Фурье (Fast Fourie Transform, см., например, Knuth 1981). Вариант данного алгоритма, применимый к квантовым вычислениям, был независимо разработан Копперсмитом (Coppersmith 1994) и Дойчем (Deutsch 1994). Его точное изложение можно также найти у Екерта и Джозса (1996), Баренцо (1996)[2]. Для перехода от уравнения (36) к преобразованию $U_{\mathcal{FF}}$ необходимо сделать упрощающее задачу предположение о том, что ω делится на r без остатка, т. е. $M = \omega/r$. Данное ограничение не искажает сути, однако при отказе от него необходимо учитывать некоторые дополнительные детали (Shor 1994, 1995, Ekert and Jozsa 1996).

Поскольку больше нет необходимости обращаться к регистру y, будем учитывать только состояние регистра x, определяемое уравнением (36).

$$U_{\mathcal{FF}} \frac{1}{\sqrt{\omega/r}} \sum_{j=0}^{\omega/r-1} |d_u + jr\rangle = \frac{1}{\sqrt{r}} \sum_k \tilde{f}(k)|k\rangle, \tag{38}$$

где

$$|\tilde{f}(k)| = \begin{cases} 1, & \text{если } k \text{ кратно } \omega/r \\ 0, & \text{во всех остальных случаях.} \end{cases} \tag{39}$$

Данное состояние проиллюстрировано на рис. 11b. Заключительное состояние регистра x теперь измерено и можно заметить, что полученное значение кратно ω/r. Остается лишь определить величину периода r. Имеем $x = \lambda\omega/r$, где λ — неизвестная величина. Если λ и r не имеют общего множителя, то нужно привести x/ω к несократимой дроби и, таким образом, определить λ и r. Если же λ и r имеют общий множитель, что маловероятно при больших значениях r, то необходимо еще раз повторить все шаги алгоритма. Можно показать, что вероятность успешного решения задачи после числа повторений, не больше (а, как правило, гораздо меньше) $\log r$, как угодно близка к 1 (Ekert and Jozsa 1996).

[2] Для осуществления точного квантового преобразования Фурье могут потребоваться операторы вращения соответственно экспоненциально точно зависящие от n. Их использование позволяет достичь эффективности решения, совпадающей с эффективностью алгоритма Шора. Однако использование приближенного варианта преобразования Фурье будет достаточным (Barenco et. al. 1996).

Квантовый алгоритм нахождения периода функции, описанный выше, может считаться эффективным, если преобразование U_f, при котором определяются значения функции $f(x)$, не является сложным. Общее количество необходимых логических гейтов полиномиально, а не экспоненциально зависит от n. Как подчеркивалось в разделе 3.2, в этом состоит главное отличие, при достаточно больших n, между разрешимыми и неразрешимыми задачами.

Для полноты описания необходимо отметить, что имеющая большое значение задача разложения на множители, которая была отмечена в разделе 3.2, может быть сведена к задаче нахождения периода простой функции. Эти и вышеуказанные сведения были впервые объединены Шором (1994). Таким образом, он показал, что задача разложения на множители может быть разрешена с помощью идеального квантового компьютера. В данном случае определяемая функция имеет вид $f(x) = a^x \bmod N$, где N — число, которое требуется разложить на множители. Значение a берется произвольно, причем $a < N$. Опираясь на элементарную теорию чисел, можно показать, что при любом a период r является четным числом, а величина $a^{r/2} \pm 1$ имеет общий множитель с N. Теперь данный общий множитель (который, разумеется, есть множитель N) может быть легко найден посредством классического алгоритма Евклида (около 300 лет до н. э., см., например, Харди и Райт (Hardy and Wright 1965)).

Для эффектного вычисления функции $f(x)$ используется повторяющееся возведение в квадрат (по модулю N): $((a^2)^2)^2 \ldots$ Затем данные степени, соответствующие двоичному разложению величины a, перемножаются. Полная сеть гейтов, необходимая для реализации алгоритма Шора, описана Микуэлем (Miquel et. al. 1996), Ведралом (Vedral et. al 1996) и Бекманом (Beckman et. al 1996) и содержит порядка $300(\log N)^3$ логических гейтов. Таким образом, для разложения на множители чисел порядка 10^{130}, предельных для современных классических методов решения, необходимо примерно $2 \cdot 10^{10}$ гейтов или 7 часов работы компьютера при «частоте переключения» 1 МГц[3]. Принимая в расчет трудности, связанные с созданием квантового компьютера, можно сказать, что данный алгоритм не обладает преимуществом перед классическими вычислениями. Однако, если увеличить число десятичных знаков до 260, то задача может считаться классически неразрешимой (см. раз-

[3]Для успешного выполнения алгоритм должен выполняться около $\log r \sim 60$ раз. Однако в среднем число необходимых выполнений гораздо меньше.

дел 3.2). С другой стороны, квантовому компьютеру для ее решения потребуется лишь в восемь раз больше времени. Существование такого мощного метода является серьезным познанием в квантовой теории.

На первый взгляд алгоритм определения периода функции похож на фокус: определение квантовым компьютером периода похоже на вынимание фокусником кролика из шляпы — не до конца ясно, как это ему удается. Анализируя рис. 11 и уравнения (34)–(38), можно сказать, что наиболее важные особенности находятся в уравнении (35). Здесь речь идет не столько об уже упомянутом *квантовом параллелизме*, сколько о *квантовом зацеплении* и, в конечном счете, о квантовой интерференции. Посредством зацепления регистров x и y, определяемое уравнением (35), каждое значение функции $f(x)$ связано со своим аргументом x. «Фокус» заключается в том, что при измерении регистра y квантовое зацепление позволяет создать в регистре x состояние $|\psi\rangle$ (уравнение (36), см. также Jozsa 1997). Заключительное преобразование Фурье может рассматриваться как интерференция различных наложенных состояний, находящихся в регистре x (сравните с действием дифракционной решетки).

Эффект интерференции может использоваться для вычислений с помощью световых или даже морских волн, т. е. он не является характерной квантовой особенностью. С другой стороны, в классических системах нельзя столкнуться с экспоненциально большими числами взаимодействующих состояний или с зацеплением.

7.3. Алгоритм поиска Гровера

Несмотря на все усилия людей, занимающихся квантовыми вычислениями, число новых практически важных алгоритмов по-прежнему мало́. Как правило, часть данных алгоритмов представляет варианты вышеуказанного алгоритма поиска периода функции. Другая часть предназначена для решения совершенно отличной от первой задачи: поиск записи в неупорядоченной базе данных (НБД). Гровер (Grover 1997) составил алгоритм для следующей задачи: дана НБД, содержащая множество записей $\{x_i\}$. Необходимо найти запись $x_i = t$. Для примера можно рассматривать поиск номера телефона в справочнике (причем имя абонента неизвестно). Нетрудно доказать, что классические алгоритмы сводятся к просмотру БД и при N записях требуют в среднем $N/2$ шагов.

Алгоритму Гровера, в свою очередь, требуется лишь $\sqrt{N}$ шагов. Данная задача, с точки зрения вычислений, по-прежнему остается сложной: ее нельзя отнести к новому классу сложности, однако, что очень важно, скорость решения даже такой, на первый взгляд, нерешаемой задачи может быть увеличена. «Квантовая скорость» $\sim \sqrt{N}/2$ превышает скорость действия алгоритма Шора по разложению на множители ($\sim \exp(2(\ln N)^{1/3})$. Она играет большую роль при наличии больших множеств ($N \simeq 10^{16}$) как, например, в случае с задачей дешифрации зашифрованных сообщений (Bassard 1997).

Важно отметить следующее: Беннетт доказал, что алгоритм Гровера является оптимальным, т.е. что ни один квантовый алгоритм не может работать быстрее, чем $O(\sqrt{N})$.

Не вдаваясь в подробности, работу алгоритма Гровера можно описать следующим образом: каждая запись имеет метку i, необходимо однозначно определить, является ли данная запись той, которую нужно найти. Другими словами, должен существовать единичный оператор S такой, что $S|i\rangle = |i\rangle$, если $i \neq j$ и $S|j\rangle = -|j\rangle$, где j — метка специально определяемого элемента. Например, проверкой необходимо определить, является ли i решением некоторой сложной вычислительной задачи[4]. Как и в случае с алгоритмом определения периода функции (уравнение (34)) данный метод начинается с представления одного квантового регистра в виде суперпозиции всех вычислительных состояний. Определим

$$|\Psi(\theta)\rangle \equiv \sin\theta|j\rangle + \frac{\cos\theta}{\sqrt{N-1}} \sum_{i \neq j} |i\rangle, \tag{40}$$

где j — метка записи $t = x$, которую предстоит найти. Данное начальное состояние $|\Psi(\theta_0)\rangle$, где $\sin\theta_0 = 1/\sqrt{N}$ является равновзвешенной суперпозицией. Затем необходимо последовательно применить оператор S, который изменит знак определяемого элемента записи на противоположный, воспользоваться преобразованием Фурье, изменить знак всех составляющих, кроме составляющей с состоянием $|0\rangle$ и вновь обратиться к обратному преобразованию Фурье. В результате данных операций может наблюдаться незначительный эффект интерференции, который приводит к следующему преобразованию

$$U_G|\theta\rangle = |\Psi(\theta + \phi)\rangle, \tag{41}$$

[4]Т.е. задач типа «NP», для которой сложно найти решение, но легко проверить правильность какого-либо предложенного решения.

где $\sin\phi = 2\sqrt{N-1}/N$. При этом коэффициент при определяемом элементе принимает несколько большее значение, чем коэффициенты при остальных составляющих. Суть данного метода заключается в повторении преобразования U_G m раз, где $m \simeq (\pi/4)\sqrt{N}$. Вследствие медленного вращения значение θ неограниченно приближается к $\pi/2$, и поэтому квантовое состояние почти абсолютно становится равным $|j\rangle$. После m повторений результатом измерения состояния становится величина j (вероятность ошибки равна $O(1/N)$). Следует отметить, что важно изначально определить значение m (это было сделано Бойером (Boyer et. at. 1996)), поскольку при увеличении числа повторений вероятность верного решения задачи снижается. Кристен Фачс (Kristen Fuchs) сравнивает данный метод с приготовлением суфле: состояние помещается в «квантовую печь», и правильный ответ начинает медленно «приготавливаться». Важно вовремя, не слишком рано и не слишком поздно, открыть печь. В противном случае приготовление суфле окончится неудачей — квантовое состояние станет ошибочным.

Два представленных алгоритма очень просты в описании. С их помощью можно проиллюстрировать разнообразие методов квантовых вычислений. Однако вопрос о существовании других методов остается открытым. Китаев (Kitaev 1996) показал решение задачи разложения на множители и сопутствующих ей посредством методики, фундаментально отличающейся от методики Шора. Метод Китаева был любезно уточнен Джозса (1997), который также показал общие черты нескольких квантовых алгоритмов, основанных на преобразовании Фурье. Таким образом, инструментарий квантового программиста постепенно увеличивается. Однако с уверенностью можно сказать, что класс задач, для которых квантовый компьютер окажется предпочтительнее классического, будет особым и, следовательно, небольшим. С другой стороны, любая задача, решение которой сложно найти, но легко проверить, может, по крайней мере, быть решена путем утомительного поиска данного решения. В этом случае алгоритм Гровера может очень пригодиться.

Глава 8

Экспериментальные процессоры, оперирующие квантовой информацией

За последние 50 лет в различных физических экспериментах были показаны наиболее элементарные квантовые логические операции. Например, операция НЕ (X) есть не что иное, как вынужденный переход между двумя энергетическими уровнями $|0\rangle$ и $|1\rangle$. Имеющая определенное значение операция XOR может быть определена как управляемый переход в четырехуровневой системе. Однако для рассмотрения работы квантового компьютера необходимо найти систему достаточно управляемую, чтобы в нужный момент задействовать какой-нибудь квантовый логический гейт, и достаточно сложную, чтобы хранить определенное количество кубитов квантовой информации.

Поиск таких систем очень сложен. Можно надеяться создать квантовые устройства на основе твердых микросхем. Это явилось бы логическим следствием развития технологии микропроизводства, которая привела к появлению современных мощных компьютеров. Однако квантовые вычисления опираются на сложные интерференционные эффекты и основной трудностью, с которой приходится сталкиваться при их реализации, являются помехи. Ни одна квантовая система не может считаться абсолютно изолированной, а ее взаимодействие с окружающей средой ведет к потере когерентности и, как следствие, к нарушению квантового вычисления. В твердых элементах роль окружающей среды играет подложка, и взаимодействие с ней очень сильно. Данное взаимодействие приводит к типичной потере когерентности через интервалы времени порядка пикосекунд. Очень важно понять, что недостаточно иметь два различных состояния $|0\rangle$ и $|1\rangle$, которые сами по себе являются стабильными (например, состояния различных токов в сверхпроводнике). Необходимо, чтобы при такой суперпозиции, как $|0\rangle + |1\rangle$ сохранялась фаза данных состояний. Однако именно в этом случае интервал времени между потерями когерентности слишком мал.

На сегодняшний день существует две перспективные системы, способные реализовать квантовое вычисление для 10–40 кубитов. Первая система была предложена Кираком и Золлером (Cirac and Zoller 1995) и заключается в использовании ряда атомов, несущих единичный элементарный заряд, помещенных в ионную ловушку и охлажденных в ее вакууме. Вторая система была предложена Гершенфельдом и Чуангом (Gershenfeld and Chuang 1997) одновременно с Кори (Cory et. al. 1996). Ее суть состоит в применении методов объемного ядерного магнитного резонанса. Оба эти предложения опираются на достойные восхищения усилия больших групп исследователей, которые разработали экспериментальные методики. Одни, более ранние предложения, касающиеся экспериментальных квантовых вычислений (Lloyd 1993, Berman et. al. 1994, Barenco et. al. 1995, DiVincenzo 1995) затрагивали другие, не менее важные методы, но являлись экспериментально нереализуемыми, другие же (Privman et. al. 1997, Loss and DiVincenzo, 1997) могут стать осуществимыми в ближайшем будущем.

8.1. Ионная ловушка

Метод ионной ловушки проиллюстрирован на рис. 12. Его подробное описание можно найти у Стина (Steane 1997). Цепочка ионов помещается в линейную «ловушку Пола» в абсолютный вакуум (10^{-8} Па) посредством комбинации статических и переменных электрических полей. Луч лазера расщепляется посредством светоделителей и акустическо-оптических модуляторов на множестве лучевых пар, каждая из которых облучает лишь один ион. Каждый из ионов может находиться в одном из продолжительных состояний, представленных, например двумя уровнями основного состояния сверхтонкой структуры (время жизни подобных состояний, в противоположность спонтанному распаду, может составлять тысячи лет). Обозначим данные состояния как $|g\rangle$ и $|e\rangle$. Они ортогональны и совместно представляют один кубит. Каждая пара лазерных лучей вызывает когерентный переход Рамана между внутренними состояниями соответствующего иона. Данная операция позволяет применить к иону любой однокубитовый, но не двухкубитовый гейт, т. к. для реализации последнего необходимо создать взаимодействие между ионами, которое обеспечивается силами электростатического отталкивания. Однако далеко не ясно, как использовать данное

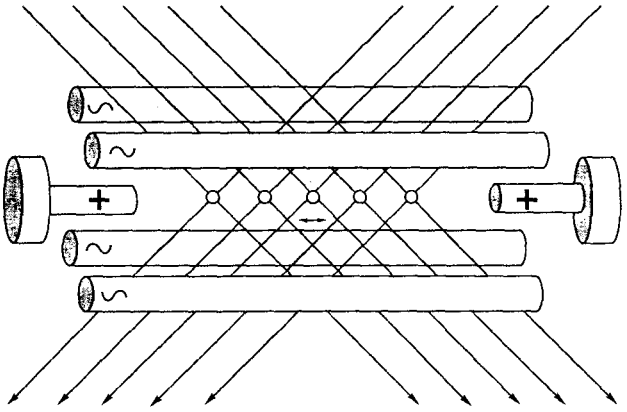

Рис. 12. Процессор (для обработки квантовой информации) на основе ионной ловушки. Цепочка атомов, несущих единичный элементарный заряд, помещена в линейную ионную ловушку. Вследствие действия электростатической силы между ионами сохраняется расстояние $\sim 20\mu$м. На каждый ион действует пара лазерных лучей, что приводит к согласованным преобразованием Рамана (Raman) и преобразованиям состояния движения цепочки. Степень свободы, определяемая движением цепочки, играет роль однобитового «транспорта», переносящего квантовую информацию между ионами. Создание какого-либо состояния осуществляется посредством оптической накачки и лазерного охлаждения; считывание информации происходит с помощью electron shelving и флуоресценции, появляющейся при резонансе. Данные способы обеспечивают высокий уровень сигнала, полученного при измерении состояния иона, по отношению к уровню помех

взаимодействие; для его объяснения от Кирака и Золлера потребуется большая проницательность.

Луч лазера переносит не только энергию, но и импульс, поэтому при взаимодействии его с ионом происходит обмен импульсами. Фактически, взаимное электростатическое отталкивание приводит к тому, что при квантовании движения вся цепочка ионов начинает двигаться *как одно целое* (эффект Мёссбауера (Mössbauer)). Движение данной цепочки является квантованным вследствие того, что она помещена в потенциал, создаваемый ловушкой Пола. Квантовые состояния движения соответствуют различным степеням возбуждения («фононам») нормальных мод колебаний цепочки. В частности, ниже будут рас-

смотрены основное состояние движения $|n=0\rangle$ и наименее возбужденное состояние $|n=1\rangle$ основной моды. С целью получения, например, операции «controlled Z» для двух ионов x и y рассмотрение необходимо начать с основного состояния движения $|n=0\rangle$. Импульс лазерных лучей, действующих на ион x, приводит к следующему переходу: $|n=0\rangle|g\rangle_x \to |n=0\rangle|g\rangle_x$, $|n=0\rangle|e\rangle_x \to |n=1\rangle|g\rangle_x$. Таким образом, к концу перехода ион находится в основном состоянии, а состояние движения совпадает с начальным состоянием иона: данное действие является операцией «обмена». Далее, импульс лазерных лучей, воздействующих на ион y, приводит к переходам:

$$
\begin{aligned}
&|n=0\rangle|g\rangle_y \to |n=0\rangle|g\rangle_y\\
&|n=0\rangle|e\rangle_y \to |n=0\rangle|e\rangle_y\\
&|n=1\rangle|g\rangle_y \to |n=1\rangle|g\rangle_y\\
&|n=1\rangle|e\rangle_y \to -|n=1\rangle|e\rangle_y.
\end{aligned}
$$

В заключении воздействуем на ион x еще одним импульсом. Общий эффект действия трех импульсов следующий:

$$
\begin{aligned}
&|n=0\rangle|g\rangle_x|g\rangle_y \to |n=0\rangle|g\rangle_x|g\rangle_y\\
&|n=0\rangle|g\rangle_x|e\rangle_y \to |n=0\rangle|g\rangle_x|e\rangle_y\\
&|n=0\rangle|e\rangle_x|g\rangle_y \to |n=0\rangle|e\rangle_x|g\rangle_y\\
&|n=0\rangle|e\rangle_x|e\rangle_y \to -|n=0\rangle|e\rangle_x|e\rangle_y,
\end{aligned}
$$

что в точности соответствует операции «controlled Z» для ионов x и y. Каждый лазерный импульс должен контролироваться по частоте и продолжительности. Операция «controlled Z» и однокубитовые гейты образуют универсальное множество и обеспечивают любые преобразования общего состояния всех ионов!

Для выполнения требований, предъявленных к квантовому компьютеру (раздел 6), необходимо создать начальное и измерить конечное состояния. Решение первой задачи возможно посредством методов оптической накачки и лазерного охлаждения. Решение второй — с помощью измерительных методик: квантового перехода, либо electron shelving.

Все данные методики являются мощными инструментами, разработанными за последние двадцать лет группами ученых, связанных

с проблемами атомной физики. Несмотря на это, одновременное применение всех методик было достигнуто экспериментально лишь единожды. В данном эксперименте было продемонстрировано измерение, создание состояния и применение квантовых гейтов для одного содержащегося в ловушке иона (Monroe et. al. 1995).

Главная экспериментальная сложность метода ионной ловушки заключается в охлаждении цепочки ионов до основного состояния ловушки (до температуры ниже одной тысячной Кельвина), а главным источником декогерентности является нагрев движения вследствие взаимодействия между ионной цепочкой, обладающей зарядом и напряжением шумов электродов (Steane 1977, Wineland et. al. 1997). Неизвестно, как сильно можно снизить нагрев. Можно считать консервативным утверждение, что за несколько лет станет возможным применять до 100 квантовых гейтов к нескольким ионам без потери когерентности. Можно надеяться, что за более длительный период оба показателя (число используемых гейтов и количество задействованных ионов) увеличится на порядок. Очевидно, что процессор, основанный на методе ионной ловушки, никогда не сможет достичь объема памяти и величины когерентности, необходимой для разложения на множители стозначного числа. Однако было бы познавательно проверить работу квантового алгоритма хотя бы на нескольких кубитах (от 4 до 10) и таким образом увидеть в действии принципы обработки квантовой информации. В разделе 9 будут показаны методы, которые позволяют значительно увеличить количество когерентных гейтовых операций.

8.2. Ядерный магнитный резонанс

Предложенный метод ядерного магнитного резонанса проиллюстрирован на рис. 13. В данном случае квантовый процессор представляет собой молекулу, «каркас» которой состоит из порядка десяти атомов. К этим атомам присоединяются другие, например, атомы водорода, так, чтобы задействовать все химические связи. Интерес в этом случае представляют ядра атомов: каждое из них обладает магнитным моментом, выраженным через спин ядра, а от состояний спина можно перейти к кубитам. Молекула помещается в объемное магнитное поле, а оперирование состояниями спина ядер осуществляется посредством контролируемых по продолжительности импульсов колеблющегося магнитного поля.

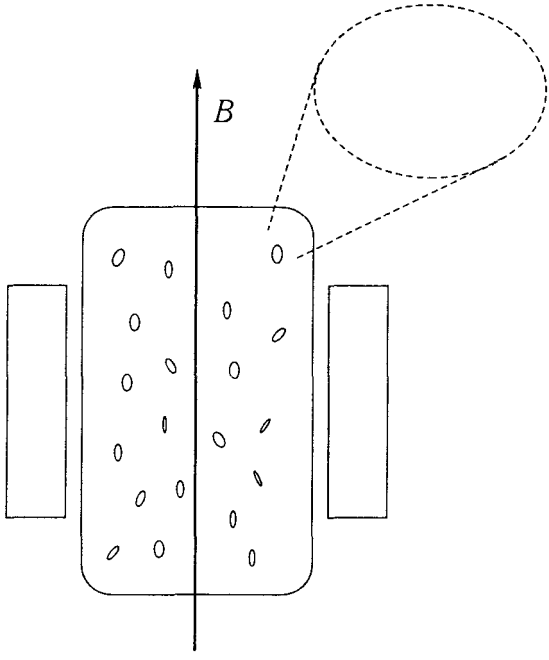

Рис. 13. Процессор (для обработки) квантовой информации, построенный на основе метода объемного ядерного магнитного резонанса. Жидкость, состоящая из $\sim 10^{20}$ «базовых» молекул, помещена в чувствительный магнитометр, который может как генерировать переменное магнитное поле, так и детектировать прецессию среднего магнитного момента жидкости. Будет неправильным полагать, что в данной ситуации задействованы 10^{20} независимых процессоров, поскольку начальное состояние соответствует термическому равновесию, а детектирование возможно лишь для усредненного конечного состояния. Оперирование и хранение информации осуществляется посредством спиновых состояний ядер. Энергетические уровни спинового состояния какого-либо ядра зависят от соседних ядер молекулы, что позволяет использовать операцию XOR. Вследствие малой величины магнитного момента ядра, энергетические уровни в некоторой степени зависят от других факторов. Из этого следует относительно медленное протекание неизбежной дефазировки процессоров по отношению друг к другу. Сама дефазировка может быть исключена посредством методики «спинового эха»

До настоящего момента не возникало никаких препятствий. Сложность заключается в том, что состояние спина ядер атомов одной молекулы не может быть ни создано, ни измерено. Для разрешения сложившейся ситуации используется некоторый объем жидкости, содержащий порядка 10^{20} молекул! Теперь становится возможным измерить усредненное получаемое состояние спина, поскольку средний колеблющийся магнитный момент всех ядер создает детектируемое магнитное поле. Здесь нужно указать несколько тонкостей. Каждая молекула жидкости имеет, вследствие влияния соседних молекул, несколько отличное локальное магнитное поле, поэтому в эволюциях каждого «квантового процессора» есть небольшие различия. Выходом здесь является использование стандартного инструмента метода ЯМР — методики спинового эха, которая позволяет нейтрализовать влияние собственной эволюции спинов, не уменьшая эффективности воздействия квантовых гейтов. Однако в этом случае возрастает сложность применения больших последовательностей квантовых гейтов. Теперь необходимо решить задачу создания начального состояния. Прежде всего отметим, что объем жидкости находится в температурном равновесии, следовательно, вероятности расположения различных спиновых состояний подчиняются распределению Больцмана. Воспользуемся тем, что энергетически спиновые состояния близки друг другу и поэтому изначально имеют примерно равное расположение. Матрица плотности ρ для $O(10^{20})$ спинов ядер близко совпадает с единичной матрицей I. Именно разность $\Delta = \rho - I$ позволяет хранить квантовую информацию. Несмотря на то, что данная разность Δ не является матрицей плотности какой-либо квантовой системы, ее возможно преобразовать путем тщательно подобранных импульсов магнитного поля тем же образом, что и матрицу плотности. Поэтому можно сказать, что она представляет собой эффективный квантовый компьютер. Подробное описание, в том числе такая особенность, как обязательное извлечение из Δ эффективного чистого состояния, выполняемого посредством последовательности импульсов, осуществляющих сжатие квантовой информации, дается Гершенфельдом и Чуангом (1997).

За несколько лет экспериментов с использованием метода ЯМР был постепенно достигнут такой уровень сложности оперирования и измерения спинового состояния, который необходим для обработки квантовой информации, представляемой несколькими кубитами. Таким образом, первый процессор, оперирующий несколькими кубитами кванто-

вой информации, будет представлять системы, работающие по методу ЯМР. Однако эффективность метода снижается при увеличении числа кубитов: например, зависимость уровня измеряемого сигнала от числа n кубитов выражается как 2^{-n}. Кроме того, существует ограничение на измерение состояния, поскольку возможно детектировать лишь усредненное состояние большого количества процессоров. Все вышесказанное ограничивает возможность использования методов исправления квантовых ошибок (раздел 9) и усложняет схемы квантовых алгоритмов.

8.3. Высококачественные оптические резонаторы

Две вышеописанные системы обеспечивают лишь обработку несложной квантовой информации, но не квантовую связь. Однако сильное взаимодействие между атомом или ионом и одиночной модой электромагнитного поля может быть получено в высококачественном оптическом резонаторе. Данное взаимодействие используется в квантовых гейтах для иона и моды поля и, таким образом, способствует передаче квантовой информации между удаленными ионными ловушками посредством высококачественных резонаторов и оптических волокон (Cirac et. al. 1997). Подобные эксперименты уже проводятся. Необходимое сильное взаимодействие между полем резонатора и атомом было продемонстрировано Бруне (Brune et. al. 1994) и Турчетте (Turchette et. al. 1995). Кроме того, электромагнитное поле может быть использовано для обеспечения взаимодействия между ионами в ловушке, являясь, таким образом, более производительной альтернативой фотонному методу (Pellizzari et. al. 1995).

Глава 9
Исправление квантовых ошибок

В разделе 7 было рассмотрено несколько достойных внимания квантовых алгоритмов. Однако в случае довольно громоздких задач, требующих тысячи кубитов и миллиарды квантовых гейтов, их быстродействие сопоставимо лишь с быстродействием алгоритмов для классических компьютеров (здесь не учитываются алгоритмы для решения задачи имитации физических систем.) После изучения в разделе 8 экспериментальных систем нужно отметить, что на данный момент возможно рассматривать «компьютеры», оперирующие лишь несколькими десятками кубитов, и, вероятно, несколькими тысячами гейтов. Их нельзя в полном смысле называть «компьютерами», поскольку они не обладают достаточно высоким уровнем сложности: в лучшем случае данные системы можно назвать скромными процессорами, оперирующими квантовой информацией. Каким образом возникло это серьезное несоответствие между желаемым и действительным?

Дело в том, что четвертый пункт требований к квантовому компьютеру, представленный в разделе 6, является физически неосуществимым. В действительности, не существует ни идеального квантового гейта, ни изолированной системы. Можно надеяться, что удастся как угодно точно приблизить реальное устройство к идеальному, но на данный момент это желание остается неосуществимой мечтой. В основе таких гейтов как XOR лежит взаимодействие двух изначально разделенных кубитов. Но если кубиты взаимодействуют друг с другом, то они неизбежно будут взаимодействовать с чем-либо еще (Plenio and Knight 1996). Необходимо упомянуть о том, что чрезвычайно сложно найти систему, в которой потеря когерентности имела бы место реже одного раза на миллион применений гейта XOR. Из этого следует, что потеря когерентности требует времени примерно в 10^7 раз меньше времени разложения на множители 130-значного числа! Еще предстоит узнать, позволяют ли законы физики очертить нижний предел скорости потери когерентности, однако уже сейчас можно с уверенностью сказать,

что легче увеличить скорость классических вычислений в 10^6 раз, чем во столько же раз снизить потерю когерентности в мощном квантовом компьютере. Данные красноречивые доказательства были представлены Гароше и Раймондом (Haroche and Raimond 1996). Их работы, как и работы Ландауера (Landauer 1995, 1996) и других можно рассматривать как предупреждение. Более подробное описание потери когерентности в квантовых компьютерах дано Унрухом (Unruh 1995), Палма (Palma et. al. 1996) и Чуангом (Chuang et. al. 1995). Серьезный численный обзор данной проблемы представлен Мигуелем (Miguel et. al. 1996) и Баренцо (Barenco et. al. 1997).

Классические компьютеры надежны не вследствие своей качественной разработки, а потому что они не чувствительны к помехам. Для того чтобы это понять, необходимо подробно изучить работу, например, триггера или обычного механического переключателя. Их устойчивость определяется комбинацией процессов усиления и рассеяния: небольшое отклонение переключателя от положения «включено» или «выключено» приводит к появлению большой возвращающей силы со стороны пружины. Ее аналогом в триггере являются усилители. Однако одной лишь возвращающей силы недостаточно: при наличии консервативной силы переключатель начнет колебаться от одного положения к другому. Не менее важно и наличие затухания, в переключателе оно обеспечивается неупругими столкновениями и, как следствие, излучением тепла. В триггере затухание реализуется за счет резисторов. Однако фундаментальные законы квантовой механики исключают перенос данных методов на квантовый компьютер. Теорема клонирования не позволяет усиливать неопределенное квантовое состояние, а диссипация несовместима с единичной эволюцией.

Такой фундаментальный подход привел к появлению широко распространенного мнения о том, что квантовая механика исключает возможность защиты квантового компьютера от случайных помех. Периодичное проецирование состояния компьютера посредством тщательно выбранных измерений само по себе не является достаточным (Berthiaume et. al. 1994, Miguel et. al. 1997). Однако с помощью тонкого использования информационной теории можно найти выход из этого тупика. Идея заключается в применении к квантовым системам методов исправления ошибок классической теории информации.

Метод исправления квантовых ошибок (QEC) был определен Стином (1996) и независимо от него Калдербанком и Шором (Calderbank

and Shor 1996) в наиболее общем виде. Они же отметили его важность. Некоторые из идей были несколько раньше высказаны Шором (1995) и Стином (1996). Данные идеи связаны с «усилением зацепления», определенным Беннеттом (Bennett et. al. 1996) и независимо Дойчем (Deutsch et. al. 1996). Теории QEC развивали Книлл (Knill) и Лафламм (Laflamme 1997), Екерт (Ekert) и Маккиавелло (Macchiavello 1996), Беннетт (Bennett, et. al. 1996). В последней работе описан оптимальный пятикубитовый код, также независимо от Беннетта открытый Лафламмом (1996). Готтесман (Gottesman 1996) и Калдербанк (1997) описали общий случай теоретического группового каркаса, из чего следовало важное понятие стабилизатора и что также способствовало определению многих новых кодов (Calderbank et. al. 1996 Steane 1996). Квантовая теория кодирования поднялась на более высокий уровень своего развития с открытием Шором и Лафламмом квантового аналога тождеств Маквильямса (MacWilliams), описываемых классической теорией кодирования. Поскольку метод QEC включает в себя применение сетей квантовых гейтов и измерений, то изначально было не ясно, должны ли данные сети быть идеальными с целью обеспечения функционирования самого метода. Важное открытие сделали Шор (1996) и Китаев (1994): они показали, как сделать сети исправления ошибок нечувствительными к ошибкам внутри данных сетей. Другими словами, подобные сети «с коррекцией ошибок» нейтрализуют помех больше, чем они создают. Методы Шора были обобщены ДиВинченцо и Шором (1996) и их эффективность была увеличена Стином (1997). Книлл и Лафламм (1996) предложили идею «вложенного» кодирования, являющуюся рекурсивным методом кодирования.

Ее суть заключается в обеспечении как угодно длительного квантового вычисления при условии нахождения отношения уровня помех к элементарной операции ниже конечного предела. Однако это преимущество метода обеспечивается за счет неэффективного использования квантовой памяти (таким образом, для его реализации необходим мощный компьютер). Данное пороговое значение величины помех было получено несколькими авторами (Knill et. al. 1996, Aharonov and Ben-Or 1996, Gottesman et. al. 1996). Более поздние методы коррекции ошибок описаны Книлом, Готтесманом и Китаевым.

Открытие метода QEC приблизительно совпало с появлением связанного с ним метода, который также обеспечивает свободную от помех передачу квантовых состояний по каналу с помехами. Речь идет

об «усилении зацепления» (Bennett et. al. 1996, Deutsch et. al. 1996). Основная идея метода заключена в том, что Алиса формирует множество зацепленных пар кубитов, а затем отправляет один кубит из каждой пары по каналу с помехами Бобу. Алиса и Боб накапливают кубиты, а затем осуществляют простое измерение с контролем по четности: например, Боб осуществляет операцию XOR для принятого и следующего за ним кубитов, а затем измеряет результирующий кубит. После того как Алиса совершит идентичные операции над своими кубитами, они сравнивают результаты. Если результаты совпадают, то можно сказать, что состояния более половины неизмеренных кубитов случайно совпадают с требуемым: $|00\rangle+|11\rangle$. Если же результаты не совпадают — кубиты отбрасываются. Посредством подобных рекурсивных проверок из множества зацепленных пар кубитов с помехами отфильтровывается несколько качественных пар. Уже обладая данным зацепленным состоянием, Алиса и Боб могут связываться посредством телепортации. Более подробное описание можно найти у Беннетта (Bennett et. al. 1996).

Опираясь на подобные идеи и значительно развив их, ван Энк (van Enk et. al. 1997) продемонстрировал способ надежной передачи квантовой информации между атомами, находящимися в удаленных друг от друга HQ оптических резонаторах посредством неидеальных оптических волокон.

Ниже в общих чертах будут показаны основные принципы QEC.

Запишем наихудший из возможных вариантов изменений, которым может быть подвержен кубит: общий случай абсолютного (т. е. полного) взаимодействия кубита с окружающей средой:

$$|e_i\rangle(a|0\rangle + b|1\rangle) \to a(c_{00}|e_{00}\rangle|0\rangle + c_{01}|e_{01}\rangle|1\rangle) + \\ + b(c_{10}|e_{10}\rangle|1\rangle + c_{11}|e_{11}\rangle|0\rangle), \quad (42)$$

где $|e_{...}\rangle$ обозначает состояния окружающей среды, а $c_{...}$ — коэффициенты, зависящие от помех. Прежде всего важно отметить, что данное выражение общего взаимодействия можно записать в следующем виде:

$$|e_i\rangle|\phi\rangle \to (|e_I\rangle I + |e_X\rangle X + |e_Y\rangle Y + |e_Z\rangle Z)|\phi\rangle, \quad (43)$$

где $|\phi\rangle = a|0\rangle + b|1\rangle$ — начальное состояние кубита, а $|e_I\rangle = c_{11}|e_{00}\rangle + c_{10}|e_{10}\rangle$, $|e_X\rangle = c_{01}|e_{01}\rangle + c_{11}|e_{11}\rangle$ и т. д. Заметим, что состояния окружающей среды не обязательно являются нормализованными. Из уравнения (43) становится ясно, что существует три основных типа ошибок,

которые необходимо исправить: X, Y и Z. Это: ошибка «переброса бита» (X), фазовая ошибка (Z) и одновременное появление данных ошибок ($Y = XZ$). Предположим, что компьютер q оперирует k кубитами квантовой информации. Пусть общее состояние k кубитов есть $|\phi\rangle$. Первым действием будет увеличение сложности компьютера и определение для последующих $n - k$ кубитов состояния $|0\rangle$. Обозначим новую систему через qc. Осуществляем операцию «кодирования»: $E(|\phi\rangle|0\rangle) = |\phi_E\rangle$. Пусть теперь помехи действуют на n кубитов системы qc. Сохраняя общность изложения, помехи могут быт представлены как набор «ошибочных операций» M, где каждая операция является тензорным произведением n операторов (один оператор на каждый кубит), выбранных из множества $\{I, X, Y, Z\}$. Например, $M = I_1X_2I_3Y_4Z_5X_6I_7$ при $n = 7$.

Общее зашумленное состояние:

$$\sum_s |e_s\rangle M_s|\phi_e\rangle. \tag{44}$$

Введем в рассмотрение еще некоторое количество кубитов: т. е. дополнительные $n - k$ кубитов, находящихся в состоянии $|0\rangle_a$. Назовем данное дополнительное множество «вспомогательным». Для любой заданной операции кодирования существует операция *определения синдрома* A, действующая на общую систему, состоящую из систем qc и a. Эффект действия данного оператора определяется как $A(M_s)|\phi_e\rangle|0\rangle_a = (M_s|\phi_e\rangle)|s\rangle_a)$ для любых $M_s \in S$. Множество S представляет собой множество исправляемых ошибок и зависит от операции кодирования. В обозначении $|s\rangle_a$, s является двоичным символом и определяет используемый оператор ошибки M_s. Как следствие, состояния $|s\rangle_a$ являются взаимно ортогональными. Для простоты изложения предположим, что общее состояние с помехами (см. уравнение (44)) содержит лишь оператор $M_s \in S$. В этом случае после операции определения синдрома системы qc и a можно представить в виде:

$$\sum_s |e_s\rangle(M_s|\phi_e\rangle)|s\rangle_a. \tag{45}$$

После этого измеряем вспомогательное состояние и получаем поразительный результат: все состояние переходит в состояние $|e_s\rangle(M_s|\phi_e\rangle_a)|s\rangle_a$ при некотором определенном значении s. В этом случае уже необходимо учитывать не общий вид помех, а лишь один определенный опера-

тор ошибки M_s. Более того, посредством данного измерения находится величина s («синдром ошибки»), с помощью которой можно определить имеющийся оператор M_s. Опираясь на полученную информацию, применим оператор M_s^{-1} к системе qc посредством нескольких квантовых гейтов (X, Y или Z), создавая, таким образом, конечное состояние $|e_s\rangle|\phi_e\rangle|s\rangle_a$. Другими словами, осуществляется восстановление состояния системы qc, свободного от помех! Конечное состояние окружающей среды является нематериальным, поэтому можно заново создать вспомогательное состояние $|0\rangle_a$ с целью дальнейшего его использования.

Выше было сделано единственное предположение о том, что помехи, определяемые уравнением (44), содержат лишь операторы ошибок, принадлежащие множеству исправляемых ошибок S. На практике, операторы ошибок могут как принадлежать, так и не принадлежать множеству S, и величина, выражающая вероятность того, что данное состояние перейдет в исправляемое после определения синдрома, имеет существенное значение. Именно здесь вступает в силу теория кодов, исправляющих ошибки: задача заключается в нахождении таких операторов кодирования и определения синдрома E, A, чтобы множество S содержало лишь исправляемые ошибки, включая все те ошибки, вероятность появления которых очень велика. Данная задача чрезвычайно сложна.

Следует отметить, что для реализации эффективной стабилизации при помехах необходимо иметь некоторую информацию о подавляемых шумах. Самым очевидным, близко соответствующим действительности предположением будет предположение о неконтролированных стохастических помехах. Другими словами, в заданное время или в заданном месте помеха оказывает какое-либо влияние, однако влияния на различные кубиты, либо на один кубит в разное время, не связаны между собой. Данное предположение соответствует квантовому эквиваленту двоичного симметричного канала, описанного в разделе 2.3. Опираясь на предположение о некоррелированных стохастических помехах, можно расположить все возможные операторы ошибки M в иерархической последовательности в зависимости от вероятности их появления, т. е. наибольшую вероятность имеют те, которые действуют на небольшое количество кубитов (т. е. лишь несколько слагаемых в тензорном произведении отличны от оператора I.) С другой стороны, наименьшую вероятность имеют операторы, действующие одновременно на большое

количество кубитов. Здесь задача заключается в нахождении таких квантовых кодов, исправляющих ошибки (QECCs), которые исправляли бы все ошибки, действующие на, максимум, t кубитов. Подобный QECC будет называться «код, исправляющий t ошибок» («t-error correcting code»).

Простейшую систему функционирования кода (предложенную Калдербанком, Шором и Стином) можно описать следующим образом. Отметим, во-первых, что такой классический код с исправлением ошибок, как код Адамара, представленный в таблице 1, может быть использован для исправления ошибок типа X. Доказательство опирается на уравнение (17), которое позволяет при операции извлечения синдрома определить вспомогательное состояние, которое будет зависеть лишь от оператора ошибки M_s, но не от состояния компьютера $|\phi\rangle$. Из этого следует, что k квантовых бита хранятся посредством 2^k взаимно ортогональных n — кубитовых состояний $|i\rangle$, где двоичное число i является членом классического кода C, исправляющего ошибки (см. раздел 2.4). Однако все вышесказанное неприменимо к исправлению ошибок типа Z. Заметим, что $Z = HXH$. Следовательно, исправление ошибок типа Z эквивалентно повороту H состояния каждого кубита, исправлению ошибок типа X и обратному вращения состояния. Данное вращение называется преобразованием Адамара и представляет лишь изменение базиса. Далее необходимо отметить следующую особенность (Steane 1996)

$$\widetilde{H}\sum_{i\in C}|i\rangle = \frac{1}{\sqrt{2^k}}\sum_{j\in C^{\perp}}|j\rangle, \tag{46}$$

где $\widetilde{H} \equiv H_1H_2H_2\ldots H_n$. Другими словами, если квантовое состояние создается путем суперпозиции всех членов классического кода C, исправляющего ошибки, то состояние, для которого было осуществлено преобразование Адамара, будет являться лишь суперпозицией всех членов двойственного кода $C^{\perp}$. Из этого следует, что после выполнения нескольких шагов при использовании квантовых состояний, описываемых уравнением (46), становится возможным исправлять и ошибки типа X, и ошибки типа Z (а следовательно, и типа Y) до тех пор, пока C и $C^{\perp}$ являются качественными кодами, исправляющими ошибки, т. е. пока оба кода обладают хорошими корректирующими способностями.

В простейшем QECC, созданном по вышеописанному алгоритму, используется $n = 7$ кубитов для сохранения одного ($k = 1$) кубита по-

лезной квантовой информации. Необходимые для хранения информации два ортогональных состояния создаются на основе кода Адамара, изображенного в таблице 1.

$$|0_E\rangle \equiv |0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle + \\ + |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle \quad (47)$$

$$|1_E\rangle \equiv |1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle + \\ + |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle. \quad (48)$$

Данный QECC обладает следующим отличительным свойством. Предположим, что состояние общего вида (оно неизвестно), содержащее один кубит, создается посредством спинового состояния $a|0_E\rangle + b|1_E\rangle$, состоящего из семи частиц со спином-$\frac{1}{2}$. Затем, над одним из семи спинов совершается какое-либо действие. Несмотря на осуществление данной операции можно по-прежнему *точно* определить первоначальное состояние кубита. Таким образом, данное серьезное возмущение никак не повлияло на хранимую квантовую информацию!

Более мощные коды QEC могут быть получены из более мощных классических кодов. Поэтому существуют более эффективные, чем описанные, конструкции квантовых кодов. Предположим, что k кубитов сохранятся посредством n кубитов. Поскольку сама ошибка может быть трех типов: X, Y или Z, то существует $3n$ вариантов появления ошибки в одном кубите. Т. к. количество битов синдрома составляет $n-k$, то (в случае если каждая ошибка одного бита, равно как и отсутствие ошибки, обладают отличными синдромами) необходимо, чтобы выполнилось неравенство $2^{n-k} \geqslant 3n+1$. При $k=1$ данное неравенство точно выполняется для $n=5$. Действительно, существует подобный пяти кубитовый код, исправляющий ошибки в одном кубите (Laflamme et. al. 1996, Bennett et. al. 1996).

В более общем случае необходимо отметить, что при фиксированном соотношении k/n существуют коды, для которых отношение t/n ограничено снизу при $n \to \infty$ (Calderbank and Shor 1995, Steane 1996, Calderbank et. al. 1997). Из этого следует квантовый вариант теоремы Шеннона (см. раздел 2.4), однако точное определение емкости квантового канала остается неясным (Schumacher and Nielsen 1996, Barnum et. al. 1996, Lloyd 1997, Bennett et. al. 1996, Knill and Laflamme 1997). При конечном n вероятность того, что помехи вызовут неисправимые

ошибки, определяется приблизительно как $(n\varepsilon)^{t+1}$, где $\varepsilon \ll 1$ — вероятность появления случайной ошибки в каждом кубите. Данное выражение определяет очень мощное подавление помех. Для эффективной работы QEC необходимо лишь уменьшить значение ε до приемлемого с помощью аппаратных средств. В качестве примера рассмотрим случай, когда $\varepsilon \simeq 0{,}001$. При $n = 23$ существует код, исправляющий ошибки в $t = 3$ кубитах (Golay 1999, Steane 1996). Вероятность появления неисправимых помех $\sim 0{,}023^4 \simeq 3 \cdot 10^{-7}$. Таким образом, подавление помех по величине составляет более трех порядков.

До настоящего момента описание QEC проводилось в предположении, что при использовании квантовых гейтов, осуществлении измерений и создания вспомогательного состояния помехи отсутствуют. Очевидно, что с целью точного описания всех возможных ситуаций, возникающих в квантовом компьютере, необходимо отказаться от данного предположения. Шор и Китаев определили методы, в которых все используемые операции реализованы таким образом, что операция исправления подавляет помех больше, чем их возникает при ее осуществлении. Основная идея здесь заключается в проверке состояний во всех случаях, где это возможно; в ограничении распространения ошибок посредством тщательного определения структуры сети и в периодичном определении синдрома: для каждой группы кубитов системы qc определение синдрома осуществляется несколько раз, а сама система qc корректируется лишь при получении $t + 1$ взаимно совместимых синдромов. На рис. 14 изображена сеть с коррекцией ошибок при определении синдрома, т. е. такая сеть, которая ограничивает распространение ошибок. Отметим, что система a проверяется перед использованием, а каждый кубит системы qc взаимодействует только с одним кубитом системы a.

При коррекции ошибок в процессе вычисления невозможно за один шаг осуществить какое-либо случайное вращение логического кубита, описываемое уравнением (33). Однако могут быть реализованы частные случаи вращения на иррациональные углы. Таким образом, посредством повторения поворотов вращение, в общем случае, определяется с любой степенью точности. Следует также отметить, что множество вычислительных гейтов является скорее дискретным, нежели непрерывным. В настоящее время были определены требования, обеспечивающие надежность квантовых вычислений при использовании QEC с коррекцией ошибок (Preskill 1997, Steane 1997). Они очень трудновы-

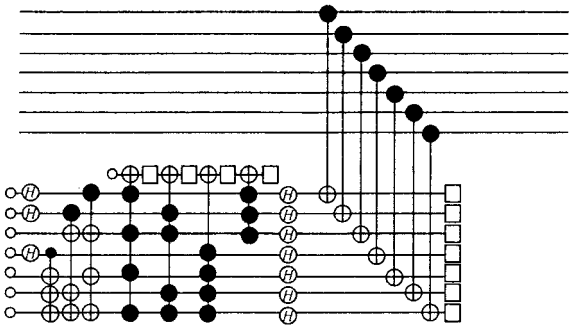

Рис. 14. Определение синдрома с коррекцией ошибок для QECC, описанного уравнениями (47), (48). Верхние семь кубитов определяют систему qc, нижние — вспомогательную систему a. Предполагается, что всем гейтам, измерениям и собственным эволюциям присущи помехи. В данном случае используются лишь гейт H и двухкубитовый гейт XOR. Если несколько гейтов XOR осуществляют идентичное управление объектным битом, то их изображения на рисунке накладываются друг на друга (NB: данное изображение не является стандартным). В первой части до изображения семи гейтов H определено создание для системы a состояния $|0_E\rangle$ и проверка самой системы: квадратный символ представляет измерение одного кубита. Если результатом какого-либо измерения будет 1, то создание состояния начнется с самого начала. Гейты H преобразуют данное состояние вспомогательной системы в состояние $|0_E\rangle + |1_E\rangle$. Окончательно, семь гейтов XOR, оперирующие кубитами систем qc и a, определяют один кубит по закодированному базису $\{|0_E\rangle, |1_E\rangle\}$. Данное действие переносит ошибки типа X из системы qc во вспомогательную систему a и ошибки типа Z в обратном направлении. Ошибки типа X, находящиеся в системе qc, могут быть определены посредством измерения системы a. Для определения ошибок типа Z необходима другая сеть. Подобные операции не подавляют все помехи в системе qc, однако их применение между операциями вычисления снижает накопление ошибок до приемлемого уровня

полнимые. Например, для вычисления, превышающего предел возможностей лучших классических компьютеров, необходимо 1000 кубитов и 10^{10} квантовых гейтов. Не используя метод QEC, потребовалось бы снизить уровень помех до порядка 10^{-13} на кубит на гейт, что является неосуществимым. С другой стороны, с использованием метода QEC необходимо повысить сложность компьютера в 10 или даже в 100 раз,

а для исправления каждого элементарного шага вычисления потребуются тысячи гейтов. Однако при этом допустимый уровень помех будет равен примерно 10^{-5} на кубит на гейт (т. е. для всех гейтов, в том числе, для гейтов, обеспечивающих исправление) (Steane 1997). Это сложно, но осуществимо.

Тот метод исправления ошибок, который в общих чертах описан в данном разделе, не является единственно возможным. При увеличении сведений о помехах более простые методы, требующие лишь несколько кубитов, могут оказаться не менее мощными. Один из таких методов был предложен Кираком (Cirac et. al. 1996). Он предназначен для подавления главного источника помех в ионной ловушке, который представляет собой изменения состояния движения во время использования гейтов. Также некоторые общие состояния могут обладать более низким уровнем помех при условии, что окружающая среда влияет сразу на все кубиты. Например, два состояния $|01\rangle \pm |10\rangle$ остаются без изменений, если воздействие окружающей среды имеет вид $|e_0\rangle I_1 I_2 + |e_1\rangle X_1 X_2$ (Palma et. al. 1996, Chuang and Yamamoto 1997). Такие состояния являются приятным исключением в хаосе потери когерентности и той квантовой информацией, содержащейся в них, можно оперировать относительно свободно. Возможно, что в реальном компьютере будет использоваться комбинация нескольких методов.

Глава 10
Обсуждение

Идея «квантовых вычислений» вдохновляла очень многих только потому, что само сочетание слов предполагает нечто удивительное, но мощное, словно физики подошли ко второй революции в обработке информации, являющейся атрибутом нового тысячелетия. Это неверное представление. Квантовые вычисления не заменят классические по той простой причине, что квантовая физика не стремится заменить физику классическую: при проектировании дома никто не консультируется у Гейзенберга (Heisenberg) и никто не отдает машину в ремонт квантовому механику. Если мощные квантовые компьютеры будут когда-либо созданы, они будут применимы лишь к тем задачам, чье решение более эффективно с точки зрения оперирования квантовой информацией.

Более серьезная причина обратиться к квантовым вычислениям заключается в том, что они способствуют более глубокому пониманию фундаментальных законов физики. Несмотря на то, что в последние годы наблюдается значительный прогресс в данной области, число ученых, занимающихся квантовыми вычислениями по-прежнему мало. Идеи классической теории информации дополняют квантовую механику и дают ощущение глубокого познания законов Природы. Теорема Шеннона о кодировании с отсутствием помех привела к появлению теоремы Шумахера и Джозса о квантовом кодировании и к определению значимости кубитов как удобной меры информации. Это позволяет отслеживать квантовую информацию и быть уверенным в том, что она не зависит от особенностей системы, в которой хранится. Необходимо также обозначить основание и других понятий, таких как «исправление ошибок» и «вычисления». Классическая теория исправления ошибок привела к появлению теории исправления квантовых ошибок. Из этого следует реализация таких физических действий, которые раньше считались неосуществимыми: в общем случае, это почти идеальное восстановление квантового состояния; преодолеваются даже такие необратимые процессы, как релаксация при спонтанной эмиссии. Например, во время длительного вычисления с исправлением квантовых

ошибок и применением методов коррекции, каждый кубит может распасться миллион раз, однако когерентность квантовой информации не будет потеряна.

Те вопросы, которые Гильберт поставил относительно логической структуры математики, побуждают задать новый вопрос о законах физики. При обращении к уравнению Шредингера не нужно упоминать, какое движение оно описывает — электрона или планеты — необходимо лишь определить допустимые данным уравнением операции над состояниями.

Язык информации и информатика позволяют связать данные вопросы с какой-либо системой отсчета. Даже простая идея квантового гейта — эквивалента классического двоичного логического гейта — имеет весьма большое значение, поскольку позволяет тщательно анализировать операции с квантовым состоянием, которые в противном случае могли бы рассматриваться как чрезвычайно сложные или непрактичные.

Идеи, подобные данной, способствуют разработке таких квантовых алгоритмов, как алгоритмы Шора, Гровера и Китаева. Данные алгоритмы показывают, что квантовая механика допускает такое оперирование информацией, какое не допускает классическая физика. Оно основано на распространении квантового состояния посредством огромного (экспоненциально большого) числа размерностей гильбертова пространства.

Результат решения проявляется вследствие контролируемой интерференции по многим вариантам вычислений. Но даже после анализа математического описания оно по-прежнему кажется необычным.

Присущая квантовым вычислениям сложность заключается в чувствительности крупномасштабной интерференции к помехам и неточностям. Часто встречается возражение, заключающееся в том, что квантовый компьютер в своей основе является скорее аналоговым, чем цифровым устройством, что, в свою очередь, ведет ко многим ограничениям. Данное мнение ошибочно. Действительно, любая квантовая система обладает непрерывным пространственным состоянием. Однако то же самое можно сказать и о любой классической системе, в том числе о цепях цифрового компьютера. Методы с коррекцией ошибок, обеспечивающие исправление ошибок в квантовом компьютере, ограничивают множество квантовых гейтов дискретным множеством. Таким образом, как и в случае с классическим цифровым компьютером, «допустимые» состояния квантового компьютера являются дискретны-

ми. Значимое различие между квантовыми и классическими вычислениями заключаются в том, что для повышения точности результата, получаемого на аналоговом устройстве, необходимо перестроить всю структуру компьютера, в то время как при использовании цифровых устройств требуется лишь увеличить число битов и операций. Невосприимчивый к ошибкам квантовый компьютер имеет больше общего с цифровым, нежели с аналоговым устройством.

Вследствие своей связи с кодированием информации, алгоритм Шора по разложению на множители стимулировал исследования в данной области. Однако мне кажется, что значимость алгоритма Шора заключается не только в его возможном использовании в отдаленном будущем для разложения на множители больших чисел. Он в большей степени является стимулом для дальнейших поисков, поскольку доказывает существование нового мощного типа вычислений, которые стали возможными, благодаря контролируемой квантовой эволюции, и вследствие того, что данный алгоритм включает некоторые новые методы вычислений. В настоящий момент большинство имеющих практическую ценность достижений в области физики квантовой информации связаны вовсе не с вычислениями, а с передачей квантового кода.

Еще двадцать лет любое экспериментально реализованное устройство не будет соответствовать термину «квантовый компьютер». Неправильное использование языка привело к тому, что любой карманный калькулятор называется «компьютером» вследствие того, что данное слово было зарезервировано для тех устройств общего назначения, которые в той или иной степени реализуют понятие Универсальной Машины Тьюринга. Для того чтобы не вводить в заблуждение, то же самое необходимо сказать и о квантовых компьютерах. Однако несложные процессоры, оперирующие квантовой информацией, могут послужить определенным целям. Например, понятия, определяемые квантовой теорией информации, позволяют получить новые эффективные методы для ядерного магнитного резонанса.

Можно обеспечить передачу квантового кода на большие расстояния и повысить ее защищенность посредством встраивания небольших «передаточных станций». Данные станции обеспечивают использование методов исправления ошибок и повышения чистоты передачи. В качестве «передаточной станции» можно использовать ионную ловушку совместно с HQ резонатором, что вполне реализуемо для данного уровня технологического развития. Безусловно, в ближайшем будущем станет

возможным осуществление очень захватывающего эксперимента — телепортации квантового состояния из одной лаборатории в другую.

Контрастом значимости сложного квантового компьютера является сложность его создания. Однако мало кто может сказать, что создание квантового компьютера не достойно тех усилий по определению недостижимости или, будем надеяться, достижимости данной задачи. Одно из главных последствий использования процессора, оперирующего несколькими квантовыми битами, — это более глубокое понимание потери когерентности в квантовой механике. Перед экспериментальными исследованиями на ближайшие несколько лет стоит следующая задача: чем жить надеждой, нужно проделать большой объем работ. С теоретической точки зрения, существует два открытых вопроса: вопрос о природе квантовых алгоритмов и вопрос об ограничении надежности квантовых вычислений. Суть квантовых вычислений до сих пор не ясна. Также пока не определен общий класс вычислительных задач, для которых посредством квантовых методов можно найти эффективное решение. Существует ли огромное число квантовых алгоритмов, которые еще только предстоит разработать, или же их количество ограничивается лишь открытыми до настоящего момента? Можно ли достичь значительной вычислительной мощности путем использования менее 100 кубитов? Ответа на этот вопрос пока не существует, поскольку на классических устройствах сложно сымитировать систему, состоящую даже из 20 кубитов. Что же касается надежности, то в этой области наблюдается значительный прогресс, и можно с уверенностью сказать, что квантовые вычисления не являются недостижимой мечтой. Сейчас можно определить требования, достаточные для обеспечения надежных вычислений, включая, например, некоррелированные стохастические помехи порядка 10^{-5} на гейт и создания квантового компьютера в сто раз сложнее того логического устройства, которое в нем находится. Однако можно ли опираться на квантовую потерю когерентности для получения свойств, принятых в подобном определении? Если нельзя, то возможно ли по-прежнему нахождение методов исправления ошибок. С другой стороны, с увеличением знаний о помехах становится возможным определение значительно сниженных требований для обеспечения надежности вычислений. В заключении хотелось бы предложить глобальную теоретическую задачу: необходимо определить несколько законов, схожих с законами сохранения энергии и момента, но используемых по отношению к информации и определя-

ющих бóльшую часть квантовой механики. Тестом для подобных идей может служить либо определяемая таким образом ясность корреляций EPR-Bell, либо точное определение данными идеями правильного использования таких терминов, как «измерение» и «знания».

Надеюсь, что физика квантовой информации определится как значительная ветвь фундаментальной физики. Задача объединения машины Тьюринга, информации, теории чисел и квантовой физики — одно из самых ярких стремлений человечества, с которой может столкнуться каждый, — является интересной для меня и, надеюсь, для читателей данного обзора.

Выражаю благодарность Royal Society и St Edmund Hall, Oxford за их поддержку.

Литература

[1] Abrams D. S. and Lloyd S. 1997 *Simulation of many-body Fermi systems on a universal quantum computer* (preprint quant-ph/9703054).

[2] Aharonov D. and Ben-Or M. 1996 *Fault-tolerant quantum computation with constant error* (preprint quant-ph/9611025).

[3] Aspect A., Dalibard J. and Roger G. 1982 *Experimental test of Bell's inequalities using time-varying analysers*, Phys. Rev. Lett. **49**, 1804–1807.

[4] Aspect A. 1991 *Testing Bell's inequalities*, Europhys. News. **22**, 73–75.

[5] Barenco A. 1995 *A universal two-bit gate for quantum computation*, Proc. R. Soc. Lond. A **449** 679–683.

[6] Barenco A. and Ekert A. K. 1995 *Dense coding based on quantum entanglement*, J. Mod. Opt. **42** 1253–1259.

[7] Barenco A., Deutsch D., Ekert E. and Jozsa R. 1995a *Conditional quantum dynamics and quantum gates*, Phys. R.ev. Lett. **74** 4083–4086.

[8] Barenco A., Bennett C. H., Cleve R., DiVincenzo D. P., Margolus N., Shor P., Sleator T., Smolin J. A. and Weinfurter H. 1995b *Elementary gates for quantum computation*, Phys. Rev. A **52**, 3457–3467.

[9] Barenco A. 1996 *Quantum physics and computers*, Contemp. Phys. **37** 375–389.

[10] Barenco A., Ekert A., Suominen K. A. and Torma P. 1996 *Approximate quantum Fourier transform and decoherence*, Phys. Rev. A **54**, 139–146.

[11] Barenco A., Brun T. A., Schak R. and Spiller T. P. 1997 *Effects of noise on quantum error correction algorithms*, Phys. Rev. A **56** 1177–1188.

[12] Barnum H., Fuchs C. A., Jozsa R. and Schumacher B. 1996 *A general fidelity limit for quantum channels*, Phys. Rev. A **54** 4707–4711.

[13] Beckman D., Chari A., Devabhaktuni S. and Preskill J. 1996 *Efficient networks for quantum factoring*, Phys. Rev. A **54**, 1034–1063.

[14] Bell J. S. 1964 *On the Einstein - Podolsky - Rosen paradox*, Physics **1** 195–200.

[15] Bell J. S. 1966 *On the problem of hidden variables in quantum theory*, Rev. Mod. Phys. **38** 447–452.

[16] Bell J. S. 1987 *Speakable and unspeakable in quantum mechanics* (Cambridge University Press).

[17] Benioff P., 1980 J. Stat. Phys. **22** 563.

[18] Benioff P 1982a *Quantum mechanical hamiltonian models of Turing machines*, J. Stat. Phys. **29** 515–546.

[19] Benioff P. 1982b *Quantum mechanical models of Turing machines that dissipate no energy*, Phys. Rev. Lett. **48** 1581–1585.
[20] Bennett C. H. 1973 *Logical reversibility of computation*, IBM J. Res. Develop. **17** 525–532.
[21] Bennett C. H. 1982 Int. J. Theor. Phys. **21** 905.
[22] Bennett C. H., Brassard G., Briedbart S. and Wiesner S. 1982 *Quantum cryptography, or unforgeable subway tokens*, in Advances in Cryptology: Proceedings of Crypto'82 (Plenum, New York) 267–275.
[23] Bennett C. H. and Brassard G. 1984 *Quantum cryptography: public key distribution and coin tossing*, in Proc. IEEE Conf. on Computers, Syst. and Signal Process. 175–179.
[24] Bennett C. H. and Landauer R. 1985 *The fundamental physical limits of computation*, Scientific American, July 38–46.
[25] Bennett C. H. 1987 *Demons, engines and the second law*, Scientific American vol. **257** №5 (November) 88–96.
[26] Bennett C. H. and Brassard G. 1989, SIGACT News 20, 78–82.
[27] Bennett C. H and Wiesner S. J. 1992 *Communication via one- and two-particle operations on Einstein–Podolsky–Rosen states*, Phys. Rev. Lett. **69**, 2881–2884.
[28] Bennett C. H., Bessette F., Brassard G., Savail L. and Sinolim J. 1992 *Experimental quantum cryptography*, J. Cryptology **5**, 3–28.
[29] Bennett C. H., Brassard G., Crepeau C., Jozsa R., Peres A. and Wootters W. K. 1993 *Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels*, Phys. Rev. Lett. **70** 1895–1898.
[30] Bennett C. H. 1995 *Quantum information and computation*, Phys. Today **48** 10 24–30.
[31] Bennett C. H., Brassard G., Popescu S., Schumacher B., Smolin J. A. and Wootters W. K. 1996a *Purification of noisy entanglement and faithful teleportation via noisy channels*, Phys. Rev. Lett. **76** 722–725.
[32] Bennett C. H., DiVincenzo D. P., Smolin J. A. and Wootters W. K. 1996b *Mixed state entanglement and quantum error correction*, Phys. Rev. A **54** 3825.
[33] Bennett C. H., Bernstein E., Brassard G. and Vazirani U. 1997 *Strengths and weaknesses of quantum computing*, (preprint quant-ph/9701001).
[34] Berman G. P., Doolen G. D., Holm D. D., Tsifrinovich V. I. 1994 *Quantum computer on a class of one-dimensional Ising systems*, Phys. Lett. **193** 444–450.
[35] Bernstein E. and Vazirani U. 1993 *Quantum complexity theory*, in *Proc. of the 25th Annual ACM Symposium on Theory of Computing* (ACM, New York) 11–20.
[36] Berthiaume A., Deutsch D. and Jozsa R. 1994 *The stabilisation of quantum computation*, in *Proceedings of the Workshop on Physics and Computation, PhysComp 94* 60-62 Los Alamitos: IEEE Computer Society Press.

[37] Berthiaume A. and Brassard G. 1992a *The quantum challenge to structural complexity theory*, in *Proc. of the Seventh Annual Structure in Complexity Theory Conference* (IEEE Computer Society Press, Los Alamitos, CA) 132–137.

[38] Berthiaume A. and Brassard G. 1992b *Oracle quantum computing*, in Proc. *of the Workshop on Physics of Computation: PhysComp'92* (IEEE Computer Society Press, Los Alamitos, CA) 60–62.

[39] Boghosian B. M. and Taylor W. 1997 *Simulating quantum mechanics on a quantum computer* (preprint quant-ph/9701019).

[40] Bohm D. 1951 *Quantum Theory* (Englewood Cliffs, N. J.).

[41] Bohm D. and Aharonov Y. 1957 Phys. Rev. **108** 1070.

[42] Boyer M., Brassard G., Hoyer P. and Tapp A. *Tight bounds on quantum searching* (preprint quant-ph/9605034).

[43] Brassard G. 1997 *Searching a quantum phone book*, Science **275** 627–628.

[44] Brassard G. and Crepeau C. 1996 SIC; ACT News **27** 13–24.

[45] Braunstein S. L, Mann A. and Revzen M. 1992 *Maximal violation of Bell inequalities for mixed states*, Phys. Rev. Lett. **68**, 3259–3261.

[46] Braunstein S. L. and Mann A. 1995 *Measurement of the Bell operator and quantum teleportation*, Phys. Rev. A **51**, R1727–R1730.

[47] Brillouin L. 1956 *Science and information theory* (Academic Press, New York).

[48] Brune M., Nussenzveig P., Schmidt-Kaler F., Bernardot F., Maali A., Raimond J. M. and Haroche S. 1994 *From Lamb shift to light shifts: vacuum and subphoton cavity fields measured by atomic phase sensitive detection*, Phys. Rev. Lett. **72**, 3339–3342.

[49] Calderbank A. R. and Shor P. W. 1996 *Good quantum error-correcting codes exist*, Phys. Rev. A **54** 1098–1105.

[50] Calderbank A. R., Rains E. M., Shor P. W. and Sloane N. J. A. 1996 *Quantum error correction via codes over* $GF(4)$ (preprint quant-ph/9608006).

[51] Calderbank A. R., Rains E. M., Shor P. W. and Sloane N. J. A. 1997 *Quantum error correction and orthogonal geometry*, Phys. Rev. Lett. **78** 405–408.

[52] Caves C. M. 1990 *Quantitative limits on the ability of a Maxwell Demon to extract work from heat*, Phys. Rev. Lett. **64** 2111–2114.

[53] Caves C. M., Unruh W. G. and Zurek W. H. 1990 comment, Phys. Rev. Lett. **65** 1387.

[54] Chuang I. L., Laflamme R., Slior P. W. and Zurek W. H. 1995 *Quantum computers, factoring, and decoherence*, Science **270** 1633–1635.

[55] Chuang I. L. and Yamamoto 1997 *Creation of a persistent qubit using error correction* Phys. Rev. A **55**, 114–127.

[56] Church A. 1936 *An unsolvable problem of elementary number theory*, Amer. J. Math. **58** 345–363.

[57] Cirac J. I. and Zoller P. 1995 *Quantum computations with cold trapped ions*, Phys. Rev. Lett. **74** 4091–4094.

[58] Cirac J. I., Pellizari T. and Zoller P. 1996 *Enforcing coherent evolution in dissipative quantum dynamics*, Science **273**, 1207.

[59] Cirac J. I., Zoller P., Kimble H. J. and Mabuchi H. 1997 *Quantum state transfer and entanglement distribution among distant nodes of a quantum network*, Phys. Rev. Lett. **78**, 3221.

[60] Clauser J. F., Holt R. A., Home M. A. and Shimony A. 1969 *Proposed experiment to test local hidden-variable theories*, Phys. Rev. Lett. **23** 880–884.

[61] Clauser J. F. and Shimony A. 1978 *Bell's theorem: experimental tests and implications*, Rep. Prog. Phys. **41** 1881–1927.

[62] Cleve R. and DiVincenzo D. P. 1996 *Schumacher's quantum data compression as a quantum computation*, Phys. Rev. A **54** 2636.

[63] Coppersmith D. 1994 *An approximate Fourier transform useful in quantum factoring*, IBM Research Report RC 19642.

[64] Cory D. G., Fahmy A. F. and Havel T. F. 1996 it Nuclear magnetic resonance spectroscopy: an experimentally accessible paradigm for quantum computing, in *Proc. of the 4th Workshop on Physics and Computation* (Complex Systems Institute, Boston, New England).

[65] Crandall R. E. 1997 *The challenge of large numbers*, Scientific American February 59–62.

[66] Deutsch D. 1985 *Quantum theory, the Church - Turing principle and the universal quantum computer*, Proc. Roy. Soc. Lond. A **400** 97–117.

[67] Deutsch D. 1989 *Quantum computational networks*, Proc. Roy. Soc. Lond. A **425** 73–90.

[68] Deutsch D. and Jozsa R. 1992 *Rapid solution of problems by quantum computation*, Proc. Roy. Soc. Lond A **439** 553–558.

[69] Deutsch D., Barenco A. and Ekert A. 1995 *Universality in quantum computation*, Proc. R. Soc. Lond. A **449** 669–677.

[70] Deutsch D., Ekert A., Jozsa R., Macchiavello C., Popescu S., and Sanpera A. 1996 *Quantum privacy amplification and the security of quantum cryptography over noisy channels*, Phys. Rev. Lett. **77** 2818.

[71] Diedrich F., Bergquist J. C., Itano W. M. and Wineland D. J. 1989 *Laser cooling to the zero-point energy of motion*, Phys. Rev. Lett. **62** 403.

[72] Dieks D. 1982 *Communication by electron-paramagnetic-resonance devices*, Phys. Lett. A **92** 271.

[73] DiVincenzo D. P. 1995a *Two-bit gates are universal for quantum computation*, Phys. Rev. A **51** 1015–1022.

[74] DiVincenzo D. P. 1995b *Quantum computation*, Science **270** 255–261.

[75] DiVincenzo D. P. and Shor P. W. 1996 *Fault-tolerant error correction with efficient quantum codes*, Phys. Rev. Lett. **77** 3260–3263.
[76] Einstein A., Rosen N. and Podolsky B. 1935 Phys. Rev. **47**, 777.
[77] Ekert A. 1991 *Quantum cryptography based on Bell's theorem* Phys. Rev. Lett. **67**, 661–663.
[78] Ekert A. and Jozsa R. 1996 *Quantum computation and Shor's factoring algorithm*, Rev. Mod. Phys. **68** 733.
[79] Ekert A. and Macchiavello C. 1996 *Quantum error correction for communication*, Phys. Rev. Lett. **77** 2585–2588.
[80] Ekert A. 1997 *From quantum code-making to quantum code-breaking*, (preprint quant-ph/9703035).
[81] van Enk S. J., Cirac J. I. and Zoller P. 1997 *Ideal communication over noisy channels: a quantum optical implementation*, Phys. Rev. Lett. **78**, 4293–4296.
[82] Feynman R. P. 1982 *Simulating physics with computers*, Int. J. Theor. Phys. **21** 467–488.
[83] Feynman R. P. 1986 *Quantum mechanical computers*, Found. Phys. **16** 507–531; see also Optics News February 1985, 11–20.
[84] Fredkin E. and Toffoli T. 1982 *Conservative logic*, Int. J. Theor. Phys. **21** 219–253.
[85] Gershenfeld N. A. aiid Chuang I. L. 1997 *Bulk spinresonance quantum computation*, Science **275** 350–356.
[86] Glauber R. J. 1986, in *Frontiers in Quantum Optics*, Pike E. R. and Sarker S., eds (Adam Hilger, Bristol).
[87] Golay M. J. E. 1949 *Notes on digital coding*, Proc. IEEE **37** 657.
[88] Gottesman D. 1996 *Class of quantum error-correcting codes saturating the quantum Hamming bound*, Phys. Rev. A **54**, 1862–1868.
[89] Gottesman D. 1997 *A theory of fault-tolerant quantum computation* (preprint quant-ph 9702029).
[90] Gottesman D., Evslin J., Kakade S. and Preskill J. 1996 (to be published).
[91] Greenberger D. M., Home M. A. and Zeilinger A. 1989 *Going beyond Bell's theorem*, in *Bell's theorem, quantum theory and conceptions of the universe*, Kafatos M, eel, (Kluwer Academic, Dordrecht) 73–76.
[92] Greenberger D. M., Home M. A., Shimony A. and Zeilinger A. 1990 *Bell's theorem without inequalities*, Am. J. Phys. **58**, 1131–1143.
[93] Grover L. K. 1997 *Quantum mechanics helps in searching for a needle in a haystack*, Phys. Rev. Lett. **79**, 325–328.
[94] Hamming R. W. 1950 *Error detecting and error correcting codes*, Bell Syst. Tech. J. **29** 147.
[95] Hamming R. W. 1986 *Coding and information theory*, 2nd ed, (Prentice-Hall, Englewood Cliffs).

[96] Hardy G.H. and Wright E.M. 1979 *An introduction to the theory of numbers* (Clarendon Press, Oxford).
[97] Haroche S. and Raimond J.-M. 1996 *Quantum computing: dream or nightmare*? Phys. Today August 51–52.
[98] Hellman M.E. 1979 *The mathematics of public-key cryptography*, Scientific American **241** August 130–139.
[99] Hill R. 1986 *A first course in coding theory* (Clarendon Press, Oxford).
[100] Hodges A. 1983 *Alan Turing: the enigma* (Vintage, London).
[101] Hughes R.J., Alde D.M., Dyer P., Luther G.G., Morgan G.L. and Schauer M. 1995 *Quantum cryptography*, Contemp. Phys. **36** 149–163.
[102] J. Mod. Opt. **41**, №12 1994 Special issue: quantum communication.
[103] Jones D.S. 1979 *Elementary information theory* (Clarendon Press, Oxford).
[104] Jozsa R. and Schumacher B. 1994 *A new proof of the quantum noiseless coding theorem*, J. Mocl. Optics **41** 2343.
[105] Jozsa R. 1997a *Entanglement and quantum computation*, appearing in *Geometric issues in the foundations of science*. Huggett S. et. al., eds, (Oxford University Press).
[106] Jozsa R. 1997b *Quantum algorithms and the Fourier transform*, submitted to Proc. *Santa Barbara conference on quantum coherence and decoherence* (preprint. quant-ph/9707033).
[107] Keyes R.W. and Landauer R. 1970 IBM J. Res. Develop. **14**, 152.
[108] Keyes R.W. 1970 Science **168**, 796.
[109] Kholevo A.S. 1973 Probl. Peredachi Inf **9**, 3: Probl. Inf. Transm. (USSR) **9**, 177.
[110] Kitaev A.Yu. 1995 *Quantum measurements and the Abelian stablizer problem*, (preprint quant-ph/9511026).
[111] Kitaev A.Yu. 1996 *Quantum error correction with imperfect gates* (preprint).
[112] Kitaev A.Yu. 1997 *Fault-tolerant quantum computation by anyons* (preprint quant-ph/9707021).
[113] Knill E. and Laflamme R. 1996 *Concatenated quantum codes* (preprint, quant-ph/9608012).
[114] Knill E., Laflamme R. and Zurek W.H. 1996 *Accuracy threshold for quantum computation*, (preprint quant-ph/9610011).
[115] Knill E. and Laflamme R. 1997 *A theory of quantum error-correcting codes*, Phys. Rev. A **55** 900–911.
[116] Knill E., Laflamme R. and Zurek W.H. 1997 *Resilient quantum computation: error models and thresholds* (preprint quant-ph/9702058).
[117] Knuth D.E. 1981 *The Art of Computer Programming*, Vol. 2: *Seminumerical Algorithms*, 2nd ed (Addison–Wesley).
[118] Kwiat P.G., Mattle K., Weinfurter H., Zeilinger A., Sergienko A. and Shih Y. 1995 *New high-intensity source of polarisation-entangled photon pairs*, Phys. Rev. Lett. **75**, 4337–4341.

[119] Laflamme R., Miquel C., Paz J. P. and Zurek W. H. 1996 *Perfect quantum error correcting code*, Phys. Rev. Lett. **77**, 198–201.
[120] Landauer R. 1961 IBM J. Res. Dev. **5** 183.
[121] Landauer R. 1991 *Information is physical*, Phys. Today May 1991 23–29.
[122] Landauer R. 1995 *Is quantum mechanics useful?* Philos. Trans. R. Soc. London Ser. A. **353** 367–376.
[123] Landauer R. 1996 *The physical nature of information*, Phys. Lett. A **217** 188.
[124] Lecerf Y. 1963 *Machines de Turing réversibles. Récursive insolubilite en $n \in N$ de l'equation $u = \theta^n u$, où θ est un isomorphisme de codes*, C. R. Acad. Francaise Sci. **257**, 2597–2600.
[125] Levitin L. B. 1987 in *Information Complexity and Control in Quantum Physics*, Blaquieve A., Diner S., Lochak G., eds (Springer, New York) 15–47.
[126] Lidar D. A. and Biham O. 1996 *Simulating Ising spin glasses on a quantum computer* (preprint quant-ph/9611038).
[127] Lloyd S. 1993 *A potentially realisable quantum computer*, Science **261** 1569; see also Science **263** 695 (1994).
[128] Lloyd S. 1995 *Almost any quantum logic gate is universal*, Phys. Rev. Lett. **75**, 346–349.
[129] Lloyd S. 1996 *Universal quantum simulators*, Science **273** 1073–1078.
[130] Lloyd S. 1997 *The capacity of a noisy quantum channel*, Phys. Rev. A **55** 1613–1622.
[131] Lo H.-K. and Chau H. F. 1997 *Is quantum bit commitment really possible?*, Phys. Rev. Lett. **78** 3410–3413.
[132] Loss D. and DiVincenzo D. P. 1997 *Quantum Computation with Quantum Dots*, submitted to Phys. Rev. A (preprint quant-ph/9701055).
[133] MacWilliams F. J. and Sloane N. J. A. 1977 *The theory of error correcting codes*, (Elsevier Science, Amsterdam).
[134] Mattle K., Weinfurter H., Kwiat P. G. and Zeilinger A. 1996 *Dense coding in experimental quantum communication*, Phys. Rev. Lett. **76**, 4656–4659.
[135] Margolus N. 1986 *Quantum computation*, Ann. New York Acad. Sci. **480** 487–497.
[136] Margolus N. 1990 *Parallel Quantum Computation*, in *Complexity Entropy and the Physics of Information, Santa Fe Institute Studies in the Sciences of Complexity.* vol. VIII p. 273 ed Zurek W. H. (Addison-Wesley).
[137] Maxwell J. C. 1871 *Theory of heat* (Longmans, Green and Co, London).
[138] Mayers D. 1997 *Unconditionally secure quantum bit commitment is impossible*, Phys. Rev. Lett. **78** 3414–3417.
[139] Menezes A. J., van Oorschot P. C. and Vanstone S. A. 1997 *Handbook of applied cryptography* (CRC Press, Boca Raton).
[140] Mermin N. D. 1990 *What's wrong with these elements of reality?* Phys. Today (June) 9–11.

[141] Meyer D. A. 1996 *Quantum mechanics of lattice gas automata I: one particle plane waves and potentials*, (preprint quant-ph/9611005).

[142] Minsky M. L. 1967 *Computation: Finite and Infinite Machines* (Prentice-Hall, Inc., Englewood Cliffs, N. J.; also London 1972).

[143] Miquel C., Paz J. P. and Perazzo 1996 *Factoring in a dissipative quantum computer*, Phys. Rev. A **54** 2605–26 I 3.

[144] Miquel C., Paz J. P. and Zurek W. H. 1997 *Quantum computation with phase drift errors*, Phys. Rev. Lett. **78** 3971–3974.

[145] Monroe C., Meekhof D. M., King B. E., Jefferts S. R., Itano W. M., Wineland D. J. alid Gould P. 1995a *Resolved-sideband Raman cooling of a bound atom to the* 3D *zero-pointenergy*, Phys. Rev. Lett. **75** 4011–4014.

[146] Monroe C., Meekhof D. M., King B. E., Itano W. M. and Wineland D. J. 1995b *Demonstration of a universal quantum logic gate*, Phys. Rev. Lett. **75** 1714–1717.

[147] Myers J. M. 1997 *Can a universal quantum computer be fully quantum?* Phys. Rev. Lett. **78**, 1823–1824.

[148] Nielsen M. A. and Chuang I. L. 1997 *Programmable quantum gate arrays*, Phys. Rev. Lett. **79**, 321–324.

[149] Palma G. M., Suominen K.-A. and Ekert A. K. 1996 *Quantum computers and dissipation*, Proc. Roy. Soc. Lond. A **452** 567–584.

[150] Pellizzari T., Gardiner S. A., Cirac J. I. and Zoller P. 1995 *Decoherence, continuous observation, and quantum computing: A cavity QED model*, Phys. Rev. Lett. **75** 3788–3791.

[151] Peres A. 1993 *Quantum theory: concepts and methods* (Kluwer Academic Press, Dordrecht).

[152] Phoenix S. J. D. and Townsend P. D. 1995 *Quantum cryptography: how to beat the code breakers using quantum mechanics*, Contemp. Phys. **36**, 165–195.

[153] Plenio M. B. and Knight P. L. 1996 *Realisitic lower bounds for the factorisation time of large numbers on a quantum computer*, Phys. Rev. A **53**, 2986–2990.

[154] Polkinghorne J. 1994 *Quarks, chaos and christianity* (Triangle, London).

[155] Preskill J. 1997 *Reliable quantum computers* (preprint quant-ph/9705031).

[156] Privman V., Vaguer I. D. and Kventsel G. 1997 *Quantum computation in quantum-Hall systems* (preprint, (iuant-pli/9707017)).

[157] Rivest R., Shamir A. and Adieman L. 1979 *On digital signatures and public-key cryptosystems*, MIT Laboratory for Computer Science, Technical Report, MIT/LCS/TR-212.

[158] Schroeder M. R. 1984 *Number theory in science and communication* (Springer – Verlag, Berlin Heidelberg).

[159] Schumacher B. 1995 *Quantum coding*, Phys. Rev. A **51** 2738–2747.

[160] Schumacher B. W. and Nielsen M. A. 1996 *Quantum data processing and error correction*, Phys. Rev. A **54**, 2629.

[161] Shankar R. 1980 *Principles of quantum mechanics* (Plenum Press, New York).

[162] Shannon C. E. 1948 *A mathematical theory of communication* Bell Syst. Tech. J. **27** 379; also p. 623.

[163] Shor P. W. 1994 *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, in Proc. 35*th Annual Symp. on Foundations of Computer Science*, Santa Fe, IEEE Computer Society Press; revised version 1995a preprint quant-ph/9508027.

[164] Shor P. W. 1995b *Scheme for reducing decoherence in quantum computer memory*, Phys. Rev. A **52** K2493–R2496.

[165] Shor P. W. 1996 *Fault, tolerant quantum computation*, in Proc. 37*th Symp. on Foundations of Computer Science*, to be published. (Preprint quant-ph/9605011).

[166] Shor P. W. and Laflamme R. 1997 *Quantum analog of the MacWilliams identities for classical coding theory*, Phys. Rev. Lett. **78** 1600–1602.

[167] Simon D. 1994 *On the power of quantum computation*, in Proc. 35*th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society Press, Los Alamitos) 124–134.

[168] Slepian D. 1974 ed, *Key papers in the development of information theory* (IEEE Press, New York).

[169] Spiller T. P. 1996 *Quantum information processing: cryptography, computation and teleportation*, Proc. IEEE **84**, 1719–1746.

[170] Steane A. M. 1996a *Error correcting codes in quantum theory*, Phys. Rev. Lett. **77** 793–797.

[171] Steane A. M. 1996b *Multiple particle interference and quantum error correction*, Proc. Roy. Soc. Loncl. A **452** 2551–2577.

[172] Steane A. M. 1996c *Simple quantum error-correcting codes*, Phys. Rev. A **54**, 4741–4751.

[173] Steane A. M. 1996d *Quantum Reed-Muller codes*, submitted to IEEE Trans. Inf. Theory (preprint quant-ph/9608026).

[174] Steane A. M. 1997a *Active stabilisation, quantum computation, and quantum state sythesis*, Phys. Rev. Lett. **78**, 2252–2255.

[175] Steane A. M. 1997b *The ion trap quantum information processor*, Appl. Phys. B **64** 623–642.

[176] Steane A. M. 1997c *Space, time, parallelism and noise requirements for reliable quantum computing* (preprint quant-ph/9708021).

[177] Szilard L. 1929 Z. Phys. **53** 840; translated in Wheeler and Zurek (1983).

[178] Teich W. G., Obermayer K. and Mahler G. 1988 *Structural basis of multistationary quantum systems* II. *Effective few-particle dynamics*, Phys. Rev. B **37** 8111–8121.

[179] Toffoli T. 1980 *Reversible computing*, in *Automata, Languages and Programming*, Seventh Colloquium, Lecture Notes in Computer Science. Vol. 84, de Bakker J. W and van Leeuwen J., eds, (Springer) 632–644.

[180] Turchette Q. A., Hood C. J., Lange W., Mabushi H. and Kimble H. J. 1995 *Measurement of conditional phase shifts for quantum logic*, Phys. Rev. Lett. **75** 4710–4713.

[181] Turing A. M. 1936 *On computable numbers, with an application to the Entschneidungsproblem*, Proc. Lond. Math. Soc. Ser. 2 **42**, 230; see also Proc. Lond. Math. Soc. Ser. 2 **43**, 544.

[182] Unruh W. G. 1995 *Maintaining coherence in quantum computers*, Phys. Rev. A **51** 992–997.

[183] Vedral V., Barenco A. and Ekert A. 1996 *Quantum networks for elementary arithmetic operations*, Phys. Rev. A **54** 147–153.

[184] Weinfurter H. 1994 *Experimental Bell-state analysis*, Europhys. Lett. **25** 559–564.

[185] Wheeler J. A. and Zurek W. H., eds, 1983 *Quantum theory and measurement* (Princeton Univ. Press, Princeton, NJ).

[186] Wiesner S. 1983 *Conjugate coding*, SIGACT News **15** 78–88.

[187] Wiesner S. 1996 *Simulation of many-body quantum system by a quantum computer* (preprint quant-ph/9603028).

[188] Wineland D. J., Monroe C., Itano W. M., Leibfried D., King B., and Meekhof D. M. 1997 *Experimental issues in coherent quantum-state manipulation of trapped atomic ions*, preprint, submitted to Rev. Mod. Phys.

[189] Wooters W. K. and Zurek W. H. 1982 *A single quantum cannot be cloned*, Nature **299**, 802.

[190] Zalka C. 1996 *Efficient simulation of quantum systems by quantum computers*, (preprint quant-ph/9603026).

[191] Zbinden H., Gautier J. D., Gisin N., Huttner B., Miiller A., Tittle W. 1997 *Interferometry with Faraday mirrors for quantum cryptography*, Elect. Lett. **33**, 586–588.

[192] Zurek W. H. 1989 *Thermodynamic cost of computation, algorithmic complexity and the information metric*, Nature **341** 119–124.

Содержание